

Submission

April 14, 2023

Department of Home Affairs
Online Webform

Re: 2023-2030 Australian Cyber Security Strategy Discussion Paper

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

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.

For the strategy to effectively improve the cyber security of Australia, the Department should consider that:

- Cyber security by design should be fostered in key software and apps markets.
- Consumers and small businesses should only have their data collected where strictly necessary and any data collected must be safely stored.
- Consumer and small business education should be a key focus of the cyber security strategy.
- Consumers should be given protections to reduce technology facilitated abuse.

Cyber security by design should be fostered in key software and apps markets

Every year the number of cyber security threats grows.¹ Many small businesses and consumers do not have the capacity to deal with complex cyber security problems as not all communications consumers possess the same level of digital ability.²

Through our engagement with consumers and small businesses, a stronger preference for cyber security by design has been expressed. Australia should adopt cyber security by design in key software market and app-development environments to facilitate improvements in cyber security at least cost to small businesses and consumers. Establishing sound baseline of cyber security for key

¹ The conversation, 2022, *Our cybersecurity isn't just under attack from foreign states. There are holes in the government's approach*, Available at: <https://theconversation.com/australia-finally-has-a-dedicated-minister-for-cyber-security-heres-why-her-job-is-so-important-184322>

² Australian Digital Inclusion Index, 2023, Key findings and next steps, Available at: <https://www.digitalinclusionindex.org.au/key-findings-and-next-steps/>

business software and apps will allow for a general uplift in cyber security, without adding undue complexity for business.³

Adopting cyber security by design would prevent many cyber security harms before they arise, saving consumers and small businesses time and money.⁴

A cyber security by design policy should be developed through consultation with community representatives. Consumer groups can provide feedback on how to develop industry wide “security by design standards”⁵ and support consumers and small businesses to adopt those standards.

Consumers and small businesses should only have their data collected where strictly necessary and any data collected must be safely stored

Privacy and data security are important to communications consumers and underpin consumers’ confidence in the communications market. Recent data breaches in the telecommunications sector have significantly reduced consumer trust in communications providers.⁶ Telecommunications providers and digital platforms should only collect consumer data where strictly necessary and must safely store the data that they collect from consumers to minimise the risk faced by consumers should a data breach occur.

Ensuring consumer privacy is protected is critical, not only to protect consumers from the material detriment they may experience, but also to protect the long-term health of digital markets. Where consumers face weak data protections, or privacy concerns they may begin to engage in behaviours to mitigate or limit their privacy risk in the event of a data breach.

Due to a lack of confidence in the security of their data, consumers may:

- Cease sharing their information and withdraw from the market entirely due to avoid the harm caused by privacy breaches.
- Create shell accounts containing limited or inaccurate personal information to avoid the harm caused by privacy breaches leading to consumer inconvenience and time cost.

Consumer and small business education should be a key focus of the strategy

The strategy should ensure that provisions for consumer education are included for consumers to effectively realise the benefits from increases in cyber security protections.

Consumer education is a critical aspect of reducing the impact of cyber harm. According to research conducted by the Consumer Policy Research Centre, 94% of surveyed consumers have high concerns about online safety issues with the highest concern being data breaches and hacks.⁷ According to the NSW government, the human element continues to drive breaches with 82% of all breaches

³The conversation, 2022, *Our cybersecurity isn't just under attack from foreign states. There are holes in the government's approach*, Available at: <https://theconversation.com/australia-finally-has-a-dedicated-minister-for-cyber-security-heres-why-her-job-is-so-important-184322>

⁴ ACCAN, 2022, *Submission to the National Security Action Plan Discussion Paper*, p.5, Recommendation 2, Available at: <https://accan.org.au/files/Submissions/2022/ACCAN%20Data%20Security%20Action%20Plan%202022.pdf>

⁵ ACCAN, 2019, *Submission to the Department of Home Affairs, Australia's 2020 Cyber Security Strategy – A call for views*, p.5, Available at: <https://accan.org.au/accans-work/submissions/1653-cyber-security-strategy>

⁶Roy Morgan, 2023, *“Telecommunications industry overtakes Social Media as the most distrusted industry”*, Available at: <https://www.roymorgan.com/findings/9193-risk-monitor-telco-most-distrusted-industry-2023>

⁷ CPRC, 2020, *CPRC 2020 Data and Technology Consumer Survey*, Available at: <https://cprc.org.au/cprc-2020-data-and-technology-consumer-survey/>

involving the use of stolen credentials, phishing or simply an error.⁸ People continue to play a large part in incidents and breaches.⁹

The strategy should consider cyber security processes to support and protect individuals and small businesses, that may not have the knowledge or digital ability to protect themselves online. The government should further invest in the creation of high quality, inclusive and accessible resources to provide consumers with personal data security skills and house those resources in a single location accompanied by a public awareness campaign.¹⁰

Consumers may experience technology facilitated abuse and should be afforded protections

Consumers may experience technology facilitated abuse through internet of things (IoT) devices, which may present risks for consumers in vulnerable circumstances. IoT devices with poor security features can leave consumers vulnerable to technology facilitated abuse and should be designed with adequate privacy and cyber security features to keep consumers safe. The strategy should ensure that a cyber secure Australia adequately engages its most vulnerable consumers in furthering their cyber protections.¹¹

Noting the harms present in online environments, the cyber security of consumers and small businesses should be a key focus of the strategy. Consumers should be sold software devices which are designed with the appropriate privacy and data protections. Consumers and small businesses should only have their data collected when strictly necessary and the data that is collected should be safely stored. Educating consumers and small businesses on cyber security and investing in digital literacy should be a key focus of the strategy.

We thank the Department for the opportunity to comment on the strategy. Should you wish to discuss any of the issues raised in this submission further, please do not hesitate to contact me at con.gouskos@accan.org.au.

The Australian Communications Consumer Action Network (ACCAN) is Australia's peak communication consumer organisation. The operation of ACCAN is made possible by funding provided by the Commonwealth of Australia under section 593 of the Telecommunications Act 1997. This funding is recovered from charges on telecommunications carriers. ACCAN is committed to reconciliation that acknowledges Australia's past and values the unique culture and heritage of Aboriginal and Torres Strait Islander peoples. [Read our RAP](#)

⁸ NSW Government, *Cybersecurity Facts*, <https://www.digital.nsw.gov.au/sites/default/files/2022-09/cyber-security-facts-poster-2022.pdf>

⁹ Ibid.

¹⁰ ACCAN, 2022, Submission to the National Security Action Plan Discussion Paper, p.5. Available at:

<https://accan.org.au/files/Submissions/2022/ACCAN%20Data%20Security%20Action%20Plan%202022.pdf>

¹¹ Research has been conducted on the regulation of internet of things devices to protect consumers as part of an ACCAN grant. The report contains 42 recommendations for legal and policy reforms aimed at addressing the distinctive features of consumer internet of things devices. Available at: <https://accan.org.au/grants/current-grants/1781-regulation-of-internet-of-things-devices-to-protect-consumers>.

Further ACCAN research on enhancing consumers awareness of privacy and the internet of things can be accessed at:

<https://accan.org.au/grants/current-grants/1611-regulating-the-internet-of-things-to-protect-consumer>