Australian Government

Australian Charities and Not-for-profits Commission

21 April 2023

2023-2030 Australian Cyber Security Strategy Discussion Paper
Department of Home Affairs

Submitted Online: 2023-2030 Australian Cyber Security Strategy Discussion Paper form (homeaffairs.gov.au)

1. The Australian Charities and Not-for-profits Commission (**ACNC**) welcomes the opportunity to comment on the 2023-2030 Australian Cyber Security Strategy Discussion Paper.

2. The ACNC recognises the importance of this conversation, and the need to ensure that Government and the private sector can support each other to ensure that information that is held virtually is secure against new and emerging threats.

About the ACNC and the charity sector

3. The ACNC is the national regulator of charities established by the *Australian Charities and Not-for-profits Commission Act 2012* (Cth) (**ACNC Act**). The objects of the ACNC Act are to:

   a. maintain, protect and enhance public trust and confidence in the Australian not-for-profit sector; and

   b. support and sustain a robust, vibrant, independent and innovative Australian not-for-profit sector; and

   c. promote the reduction of unnecessary regulatory obligations on the Australian not-for-profit sector.

4. Currently, the ACNC has oversight of around 60,000 registered charities. These charities vary considerably in size, role, and function. Charities are a vital part of our community and economy. Registered charities employed over 1.3 million people[1] and reported revenue of $176 billion in the 2020 reporting period.[2] While some charities are large and well-known entities, most charities are very small, volunteer-run organisations.[3]

[1] Australian Charities and Not-for-profits Commission, Australian Charities Report – 8th edition, 2022, 13.
[2] Australian Charities and Not-for-profits Commission, Australian Charities Report – 8th edition, 2022, 14.
[3] Australian Charities and Not-for-profits Commission, Australian Charities Report – 8th edition, 2022, 7; 11-13.

GPO Box 5108 Melbourne VIC 3001
Tel 13 ACNC Fax 1300 232 569
acnc.gov.au

Cyber security and the charity sector

5. We note the discussion paper is seeking to identify solutions that governments can adopt to uplift cyber security and resilience "across the digital economy". Charities are a vital part of the national economy, and increasingly hold information and engage digitally (including, for example, by the use of online fundraising platforms).

6. Charities must be considered in any reforms, as part of the wider economy. That consideration should include that aspects of charities' needs and interests may differ from other parts of the private sector.

7. Many charities hold significant amounts of sensitive personal information about Australians because they are engaged by government to deliver services such as social welfare, aged care, education and medical treatment. In the 2020 reporting period, registered charities received $88.8 billion in revenue from government.[4]

8. Charities that raise funds from the public[5] hold sensitive financial details of donors and individual and corporate philanthropists, such as credit card details. This may make some charities attractive targets for cyber security attacks.

9. Furthermore, the impact of a cyber security attack on a charity may have implications on public trust and confidence on the charity sector as a whole. In 2022 The Smith Family was the subject of a cyber-attack attempting, but failing, to access donor funds. However, The Smith Family thought hackers may have had access to the personal information of donors during the cyber-attack. The resulting media headlines illustrate the impact such an attack can have on the sector as whole.[6]

10. Over 51% of charities operate without paid staff.[7] Many more charities are reliant on part-time workforces and may have less capacity to invest time in training and embedding cyber security consciousness in their staff than other private sector

[4] Australian Charities and Not-for-profits Commission, Australian Charities Report – 8th edition, 2022, 19. Note that this amount includes JobKeeper payments made during the reporting period.
[5] For the 2021 reporting period, charities reported to the ACNC that they received $13.4 billion from donations and bequests.
[6] Avantika Chopra, 'Australia Again! The Smith Family Data Breach Could Gravely Impact Donors', *Firewall Daily* (online, 22 November 2022) < The Smith Family Cyber Attack May Put 80,000 Donors At Risk (thecyberexpress.com)>; Warren Barnsley, 'The Smith Family warns supporters of stolen personal data amid hack on Australian charity', *7 News* (online, 22 November 2022) < The Smith Family warns supporters of stolen personal data amid hack on Australian charity | 7NEWS>; Padraig Collins, 'Not even charities are safe anymore: Hackers target The Smith Family with credit card details and phone numbers stolen in the cyber attack', *The Daily Mail Australia* (online, 22 November 2022) < Smith Family charity cyber attack compromises credit card details and phone numbers | Daily Mail Online>.
[7] Australian Charities and Not-for-profits Commission, Australian Charities Report – 8th edition, 2022

organisations. Part-time and volunteer workforces are also less likely to absorb and retain information about cyber security procedures.[8]

11. In a tight funding environment and being purpose-driven, charities may have difficulty in deciding to divert money toward cyber security measures that would otherwise be spent on directly furthering their charitable purposes.[9]

12. A recent report from the United Kingdom focussed on the cyber threats facing charities found:

    a. Charities are less likely to have expertise in-house to embed and manage systems to defend against cyber attacks due to lack of resources and/or specialist IT skills and knowledge.[10]

    b. Charities are more likely to rely on staff using their own IT equipment for work purposes due to lack of resources, which is more difficult to secure and manage than enterprise IT systems.[11]

    c. Due to limited resources and capability, charities are likely to be less resilient in the event of a cyber security incident to respond to and recover from an incident.[12]

13. The discussion paper notes that "stakeholders have encouraged government to streamline reporting obligations and response requirements following a major cyber incident". Any steps to ease this potential burden for charities would align with the object of the ACNC Act to reduce unnecessary regulatory obligations for charities. However, when charities report cyber security incidents, it is important that consideration is given to providing the charity (and other similar charities) with guidance and support to efficiently uplift their security standards and mitigate the risks arising from the incident.

14. Where regulatory reform occurs, harmonisation across existing frameworks should be considered in designing those changes. The ACNC is committed to working across government to assist in harmonising state and territory regulations that impact charities because it enhances the viability and efficiency of the sector. In the context of regulatory reforms to improve cyber security, consistent language and objectives across

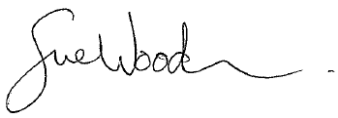
[8] Our Community Pty Ltd, *Damn Good Advice On Cyber Safety and Fraud Prevention* (Report, July 2019) 30-31.
[9] Social Ventures Australia, *Paying what it takes: Funding indirect costs to create long-term impact* (Report, March 2022) 39-40 ; National Cyber Security Centre, *Cyber threat report: UK charity sector* (Report, January 2023) 7.
[10] National Cyber Security Centre, *Cyber threat report: UK charity sector* (Report, January 2023) 7; Infoxchange, *Digital Technology in the Not-for-Profit Sector* (Report, November 2022) 11.
[11] National Cyber Security Centre, *Cyber threat report: UK charity sector* (Report, January 2023) 7.
[12] National Cyber Security Centre, *Cyber threat report: UK charity sector* (Report, January 2023) 8.

Commonwealth legislation and frameworks is vital, as is acknowledgment of existing international frameworks (recognising that a number of charities operate internationally), where appropriate.

15. For example, the Department of Employment and Workplace Relations (**DEWR**) uses an External Systems Accreditation Framework and a 'Right Fit For Risk' assurance approach to ensure that external IT systems and providers of its services have adequate data protection measures in place.[13] Providers, many of whom are charities, must complete a process with three milestones, which include assessing their level of cyber security in place, implementing any improvements identified and implementing a customised Information Services Management System (ISMS) that conforms with ISO 27001, a best practice standard for ISMS.[14] This process is labour and resource-intensive. We understand that other government funders may have their own frameworks, therefore charities that receive funding from multiple departments currently may have to meet multiple cyber security standards to receive funding to provide services. Further, if the DEWR framework were a national standard for all charities, many would face difficulty complying without assistance.

Next steps

16. If you have queries about this submission please contact Joanna Austin, Director, Legal and Policy by email at joanna.austin@acnc.gov.au.



Sue Woodward AM
Commissioner
Australian Charities and Not-for-profits Commission

[13] Accreditation overview - Department of Employment and Workplace Relations, Australian Government (dewr.gov.au).
[14] Process for accreditation - Department of Employment and Workplace Relations, Australian Government (dewr.gov.au).