8 November 2019.

Department of Home Affairs
3 Lonsdale St,
Braddon ACT 2612

Dear Sir/Madam,

NetThing submission to the Department of Home Affairs call for views: *Australia's 2020 Cyber Security Strategy*.

NetThing welcomes the opportunity to provide a submission to the Department of Home Affairs' call for views on *Australia's 2020 Cyber Security Strategy*.

Cyber security has never been more important. As our lives and economy increasingly shift 'on-line', the risk to our prosperity and way of life is real, and we need to ensure an appropriate and flexible strategy is in place to manage both current and future risks that does not simultaneously expose Australians to increased risk arising from a desire to increase surveillance capabilities to protect national security.

We wish to make one brief point in relation to Australia's 2020 Cyber Security Strategy, which is the inherent conflict of interest that exists where the government agency responsible for surveillance and national security is simultaneously responsible for cyber security.

Inherent conflict of interest

There is an inherent conflict of interest where the government agency responsible for surveillance and national security is simultaneously responsible for cyber security. The government has the accountability to drive cyber resilience across the whole of the economy, including critical infrastructure, systems of national interest, federal, state and local governments, small and medium business, academia, the not-for-profit sector and the Australian community[1]. At the same time, the government is also the actor called upon to re-establish control over the misuse of cyberspace, including developing tools and capabilities to conduct surveillance and potentially cyber offensive strikes against rogue actors.

[1] ACSC role. https://www.asd.gov.au/cyber

While it is clear these two roles must coexist within the one government, it is vital that accountability for the two roles is separated to ensure informed debate within government and the creation of policies that result in the best outcomes for all Australians. Unfortunately, this is not the case in Australia where the responsibility for driving cyber resilience resides with the Australian Cyber Security Centre (ACSC) which is part of the Australian Signals Directorate (ASD), while the ASD is simultaneously responsible for cyber offensive activities.

This conflict of interest extends to DoHA, where they are simultaneously responsible for weakening the security of cyber infrastructure, through the creation of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (TOLA), while having the accountability for the current call for views on Australia's 2020 Cyber Security Strategy. TOLA, as written by Department of Home Affairs (DoHA), provides exceptional access to encrypted data by law enforcement. Exceptional access creates systems that are inherently less secure, more expensive, and more complex. Exceptional access also diminishes trust in government by the Australian community, and lessens trust in Australian ICT chains, compared to products supplied by jurisdictions without exceptional access regimes. There is room for improvement, and the paper **Keys under the Doormat** in the Journal of Cybersecurity[2] provides valuable insight to the inherent risks associated with exceptional access.

In order to separate the accountability for developing Australia's 2020 Cyber Security Strategy from the agency responsible for the TOLA legislation and cyber offensive activities, we recommend an appropriate government agency to define and manage Australia's Cyber Security Strategy is the ACSC. While we realise ACSC resides under ASD, moving the accountability for Australia's cyber security strategy to ACSC will ensure the strategy can be developed at arm's length from the areas of ASD responsible for cyber offense and from DoHA, which will lead to informed debate about the merit of various approaches. This in turn will ensure that agencies responsible for national security are less likely to undermine cyber security to the betterment of all Australians.

Peter Tonoli,
NetThing committee member, on behalf of the NetThing Cyber Security Panel

[2] Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., ... & Rivest, R. L. (2015). Keys under doormats: mandating insecurity by requiring government access to all data and communications. Journal of Cybersecurity, 1(1), 69-79. Available at https://www.cl.cam.ac.uk/~rja14/Papers/doormats.pdf

About NetThing

NetThing is the renewal of an annual forum to strengthen Australia's Internet governance community, and consists of robust Australia-based Internet policy exploration and discussion. Over time we aim to become the re-birthed, reinvigorated Australian connection to the Internet Governance Forum[3].

This annual forum will focus on:

- Building a diverse and inclusive Internet governance community in Australia.
- Exploring national and international Internet governance policy issues.
- Sharing technical expertise and policy understanding in a way that people with less technical experience can understand and relate to.
- Acting as an apolitical and non-partisan forum advocating the benefits of the Internet and related services and technologies.

It functions as a symposium where a diversity of views and perspectives are shared but will not itself seek to formulate final positions or make decisions.

[3] https://www.intgovforum.org/multilingual/