Electronic Frontiers
AUSTRALIA

W www.efa.org.au
E email@efa.org.au
@efa_oz

8 November 2019

The Hon Peter Dutton MP
Minister for Home Affairs
Shop 3/199 Gympie Rd
STRATHPINE QLD 4500

By eLodgment

Dear Minister,

RE: AUSTRALIA'S 2020 CYBER SECURITY STRATEGY

We appreciate this opportunity to make submissions in relation to Australia's 2020 Cyber Security Strategy.

EFA's submission is contained in the following pages and we appreciate the brief extension of time to provide this submission by 8 November 2019.

Established in January 1994, EFA is a national, membership-based non-profit organisation representing Internet users concerned with digital freedoms and rights. EFA is independent of government and commerce, and is funded by membership subscriptions and donations from individuals and organisations with an altruistic interest in promoting civil liberties in the digital context.

EFA members and supporters come from all parts of Australia and from diverse backgrounds. Our major objectives are to protect and promote the civil liberties of users of digital communications systems (such as the Internet) and of those affected by their use and to educate the community at large about the social, political and civil liberties issues involved in the use of digital communications systems.

Yours sincerely,

[redacted]

Angus Murray
Chair of the Policy Committee
Electronic Frontiers Australia

Submissions

1. Where appropriate, we have specifically responded to the call for views contained at pages 19 to 21 of the Australia 2020 Cyber Security ("**the Strategy**") in the following paragraphs.

2. At the outset, and in the interest of ensuring that the subsisting position of Electronic Frontiers Australia is made abundantly clear in this submission. That position is that Australians ought to be afforded the benefit of a base-line safeguard for human rights protection in the form of a Federal enforceable human rights framework.

3. In our view, the justification of increased surveillance and law enforcement powers cannot be justified without the existence of a Federal enforceable human rights framework and that current and future legislation ought to be subject to the Court's scrutiny through an enforceable and actionable lens of human rights compatibility.

What is your view of the cyber threat environment?

4. It is unfortunate that malicious operators exist and that a loss has, and is being, caused to the detriment of ordinary Australians as a consequence of the proliferation of technology. However, this risk should not result in the degradation of fundamental human rights including the right to association, privacy, political opinion and free speech.

5. In our view, this is a multi-facetted issue that affects business, government and individuals and individual rights ought to remain paramount to understanding the cyber threat environment.

6. We do not consider that "whack-a-mole" responses such as website blocking or excessive intrusions into Australians' private lives are a proportionate response to the threat environment and we strongly urge the Australian government to explore educational options as well as protecting Australians' rights via a Federal and enforceable human rights framework.

What threats should Government be focusing on?

7. Government should focus on alerting people to cyber threats, empowering people to manage their risk to cyberthreats and being proactive to help people put better systems in place for their own cyber security. For individuals this may look like widespread campaigns to warn people of phishing attacks and assistance with keeping software up to date and personal details private. For businesses, notification of suspicious traffic from online systems with assistance for clearing hacks would be useful.

8. Government, through the Cyber Security Centre or similar, should be proactive about alerting and assisting businesses and individuals.

9. Government should also be working with large industries to plug gaps that facilitate cyber fraud. For example; tightening credit card security, tightening paypal transactions, ensure banks report suspicious transactions, holding social media companies to account for content and advertising posted on their networks.

Do you agree with our understanding of who is responsible for managing cyber risks in the economy?

10. We believe that government should focus on maintaining government cyber security and regulating non-government entities so as to enforce better cyber security practices.

11. Government provides critical and sensitive services to Australians and if those services were perceived to be vulnerable to cyber attacks, this could significantly undermine the government's work and social license to operate. Accordingly, we are of the view that steps should be taken to ensure that all departments meet a minimum level of cyber security, such as that provided by the Essential Eight, that industry be required to meet similar standards and that recommendations in past enquiries, such as the Digital Platforms enquiry and the past Australian Law Reform Commission into digital services and privacy should be reviewed and implemented.

Do you think the way these responsibilities are currently allocated is right?

12. In our view, the government ought to ensure that Australians are provided with base-line protections and are properly informed as to the existence of these protections. This includes, for example, a human rights framework and an education campaign commitment to ensuring that Australians are empowered to identify cyber security threats and form informed opinions.

What changes should we consider?

13. We repeat that Australia ought to introduce an enforceable human rights framework as the first and most critical aspect of protecting Australians.

14. Secondly, we recommend that the Government commits to:

    a. Properly consulting with industry and civil society when considering the introduction of cyber-security and national security legislation rather than rushing legislation[1]; and

[1] See for example: *Telecommunications and Other Legislation (Assistance and Access) Bill 2018* introduced on 20 September 2018 and, despite the Parliamentary Joint Committee on Security and

b. Budget for an education campaign targeted to all facets of Australian society to inform and properly equip Australians with an understanding of their rights and digital literacy.

What role should Government play in addressing the most serious threats to institutions and businesses located in Australia?

15. We refer to our responses to previous questions and add that significant improvements can be made in improving public cyber security awareness. Improved digital literacy would not only improve Australia's overall security but also its competitiveness on the international market. There are several challenges that cyber security awareness campaigns experience:

    a. reaching consumers that may not be interested in cyber security and have low literacy;
    b. ensuring consumers remain up-to-date and apply their cyber security skills in both their personal and professional lives; and
    c. providing cyber security training at a level that is engaging and helpful to both new listeners and more experienced listeners.

16. A measure to ensure future generations, which natively use technology, are protected online, even from a young age, would be to include computing, programming and cyber security skills in primary and secondary education curriculums.

17. Furthermore, we believe that the EU initiative *Digital Opportunities*, the aim of which is to give students of all disciplines the opportunity to get hands-on digital experience in fields demanded by the market, is a good example of how digital skills could be improved in the current workforce. The government should also consider a national initiative for industry-based learning in digital fields as well as promoting opportunities for mature Australians to retrain or learn additional digital skills to promote their own competitiveness and digital literacy.

18. Implementing all of the above would go a long way in ensuring that Australians are consistently provided with opportunities, both voluntary and compulsory, to improve their digital literacy, and would over time raise the baseline cyber security awareness across the nation.

How can Government maintain trust from the Australian community when using its cyber security capabilities?

19. We respectfully repeat that the Australian community ought to be afforded the protection in the form of an enforceable federal human rights framework.

Intelligence having yet to release its Report and a *seriously* abridged submission timeframe, passed on 8 December 2018.

20. More specifically in response to the question, trust is built from transparency and respect. In our view, the Australian government needs to build trust by *clearly* separating cyber-security from the national security rhetoric. These are two fundamentally different concepts and should not be confused.

What customer protections should apply to the security of cyber goods and services?

21. Australians should not be subjected to cyber goods and services that are exposed to covert surveillance and the *Telecommunications and Other Legislation (Assistance and Access) Bill 2018* should be repealed.

What role can Government and industry play in supporting the cyber security of consumers?

22. Government could fund a cyber security audit service for businesses and individuals, with vouchers to fund IT experts to update systems and educate people about threats and scams.

How can Government and industry sensibly increase the security, quality and effectiveness of cyber security and digital offerings?

23. We repeat the importance of education and digital literacy.

Are there functions the Government currently performs that could be safely devolved to the private sector?

24. No comment.

What would the effect(s) be?

25. No comment.

Is the regulatory environment for cyber security appropriate? Why or why not?

26. We respectfully repeat that an enforceable federal human rights framework is necessary to safe-guard Australians' fundamental freedoms and, with respect, the consultation appears to inappropriately blur cyber-security with national security making this question difficult, if not impossible, to meaningfully answer.

What specific market incentives or regulatory changes should Government consider?

27. No comment, noting our submissions above.

What needs to be done so that cyber security is 'built in' to digital goods and services?

28. An increased focus on the principle of privacy by design and protection of fundamental human rights.

How could we approach instilling better trust in ICT supply chains?

29. No comment.

How can Australian governments and private entities build a market of high quality cyber security professionals in Australia?

30. The government could support existing industry based certification bodies such as CREST. Support for existing educational courses run by tertiary institutions and TAFEs, and acknowledge that the current high demand for professionals in these areas may require special arrangements such as salary supplements and industry co-operation. Create a replacement program similar to the previous Cyber Security Small Business Program[2], but including non-profit organisations.

Are there any barriers currently preventing the growth of the cyber insurance market in Australia? If so, how can they be addressed?

31. Insurance is a valuable part of a risk management strategy. The government should ensure that there are incentives to link the insurance and security industries closely so that insurance is not simply a financial risk management technique, but is linked to genuine improvement of security — cyber insurance must be a driver of improved security practices, not a way for industry to buy their way out of data breach risks.

How can high-volume, low-sophistication malicious activity targeting Australia be reduced?

32. Attempts to block high volume malicious attacks, like email scams, result in increasingly sophisticated attacks to circumvent the blocks. Public education about how attacks work and what to look out for are preferable.

What changes can Government make to create a hostile environment for malicious cyber actors?

33. EFA does not believe that the non-military sector of the Australian Government should be involved in prosecuting offensive cyber operations, nor private citizens or enterprise. Offensive operations should solely be delegated to the Australian Defence Force. Civilian involvement in offensive cyber actions brings upon the risks of miscalculation, escalation in offensive operations, and breach of the

[2] https://www.business.gov.au/assistance/cyber-security-small-business-program

territoriality of other states. Furthermore, civilian possession of offensive technologies further perpetuates proliferation of offensive cyber technology, and increases the chances that those technologies could get into the possession of Australia's adversaries.

34. The best form of providing a hostile environment for malicious cyber actors, is one that is difficult and expensive, in time and money, to compromise by those actors. The ubiquitous use of strong encryption is integral for protecting infrastructure and data from malicious actors. Strong encryption increases the difficulty, and cost, to malicious actors, in their attempts to compromise infrastructure and data. The measures legislated in *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, which subverts protection provided by encryption, is antithetical to providing the utmost protection to infrastructure and data, and, therefore, diminishes the robustness of hostile environments to malicious cyber actors. Compromised encryption technology, as mandated by TOLA, increases the risks that confidentiality and integrity of data will be breached. The same measures that weaken encryption, in the name of law enforcement, can also be used by malicious actors, to their advantage, at the detriment of their victims.

How can governments and private entities better proactively identify and remediate cyber risks on essential private networks?

35. No comment.