Our Ref
EK

Your Ref

1 November 2019

Cybersecurity Policy Review

To whom it may concern

Australia's 2020 Cyber Security Strategy - Submission

I make this submission on my own behalf and on behalf of Cooper Mills Lawyers.

Firstly, I would like that thank the Department for an invitation to participate in the recent focus group.

Cooper Mills Lawyers has significant involvement in the cybersecurity industry including representing some of the nation's leading service providers.

It is critical that the review be used to identify areas for continuous improvement and make the 2020 Policy even more effective than the 2016 Policy.

There are three areas where I see considerable thought needs to be focused on:

1. Critical Infrastructure;
2. Education and training;
3. Information collection and management;

For the purposes of this short submission I will only address the first issue in so far as it relates to the Australia domain name system (**DNS**).

Critical Infrastructure

Effective oversight of critical infrastructure is an essential element of any cyber strategy, yet one of the biggest pieces of critical infrastructure is still operated as private company limited by members guarantee. .au Domain Administration Ltd (**auDA**) is the industry self-regulatory body that administers the .au domain name space, which underpins much of Australia's digital economy.

auDA is currently overseen by the Department of Communications and the Arts (**DOCA**) who approach that oversight role from an internet governance perspective, while that is important, times have changed, and the DNS is no longer something that should be viewed solely through that lense. DNS is now at the forefront of cybersecurity in Australia, it is particularly relevant as a probable attack vector, predominantly by foreign state actors. Examples of this exist, such the massive attack on the .TR ccTLD in 2015[1].

While auDA does engage with Federal Agencies its falls outside of the Department of Home Affairs (**Home Affairs**) which is tasked with management of Australia's cybersecurity strategy. It is our submission that oversight of auDA is better managed by Home Affairs rather than DOCA. A reassignment of the oversight role by Home Affairs would include numerous benefits such as:

[1] Details of the attack are set out here - https://ccnso.icann.org/sites/default/files/field-attached/presentation-tr-ddos-attack-07mar16-en.pdf

www.coopermills.com.au

LEVEL 8, 410 COLLINS ST
MELBOURNE VIC 3000
AUSTRALIA

GPO BOX 648
MELBOURNE VIC 3001
AUSTRALIA

TEL +61 3 9866 8850
FAX +61 3 8679 3350
INFO@COOPERMILLS.COM.AU

1. Allow better coordination within the Home Affairs portfolio of national security and law enforcement agencies;
2. Allow a more consistent approach to cybersecurity;
3. Allow Home Affairs to benefit from auDA's self-funding and substantial financial resources in rolling out security measures to protect the Australian DNS;
4. Provide auDA with substantial resources and skills from within Home Affairs that may not necessarily be present in DOCA;

I am happy to discuss any aspect of this submission further.

Yours faithfully,
COOPER MILLS LAWYERS

Erhan Karabardak
Legal Practitioner
Registered Trade Marks Attorney
[redacted]