THE LAW SOCIETY
OF NEW SOUTH WALES

Our ref: PuLC:EEce: 1790282

1 November 2019

Cyber Security Policy Division
Department of Home Affairs
PO Box 6022
Parliament House
Canberra ACT 2600

Dear Sir/Madam,

Australia's 2020 Cyber Security Strategy

The Law Society of NSW appreciates the opportunity to provide a submission to the Department of Home Affairs consultation on Australia's 2020 Cyber Security Strategy. This submission has been informed by the Law Society's Public Law and Legal Technology Committees. Lawcover has also contributed to components of this submission, as indicated below. Lawcover is the single provider of approved professional indemnity insurance policies to law practices based solely in NSW and is a wholly owned but independent subsidiary of the Law Society. This submission addresses the issues raised in the *Australia's 2020 Cyber Security Strategy – A call for views* discussion paper ("the discussion paper") in two parts.

Firstly, we respond to discussion questions of particular interest to the Law Society. Our views on these questions are informed by the circumstances of legal practice in firms, courts and online as well as by the legal profession's ethical obligations and fiduciary relations. Cyber threats challenge how these issues are securely, efficiently and effectively managed in a digital environment. On this basis, it is submitted that the Government must support measures to protect the integrity of this interconnected ecosystem by ensuring the safety, privacy and security of all involved.

Secondly, our submission considers the broader national security issue of offensive cyber operations ("OCOs"). The Law Society submits that whilst OCOs can help to protect Australia's national interests, their use has significant implications and should only be used with proportionality in situations of necessity. The current Cyber Security Strategy should be further developed to provide a robust, unambiguous policy and legal framework regarding the use of OCOs.

Responses to the *Australia's 2020 Cyber Security Strategy – A call for views* discussion questions

1. *What is your view of the cyber threat environment? What threats should Government be focusing on?*

Cyber threats, including data and privacy breaches, malware and ransomware attacks and identity fraud, are widespread issues. As with the broader community, the legal profession faces an array of cyber threats which impact on practice and procedure with respect to insurance, data storage, funds transfers and electronic communications. Cyber threats that

impact the profession can undermine the confidentiality of the relationship between solicitor and client and reduce the level of trust which business and the community place in the profession. In this regard, the International Bar Association has noted that data breaches can have dire consequences for client confidentiality, reputation, financial dealings and commercial interests.[1]

The Law Society is of the view that the cyber threat environment is a shared problem requiring Government intervention, which could include training, information dissemination, and product and services standards. We note that the National Cyber Security Centre in the UK offers segment-focussed guidance such as threat assessments, weekly threat reports and incident trends reports. Having information targeted to different roles in the economy can enhance the educative process. Government also has an interest in supporting the security of legal practice as law firms hold large volumes of valuable personal and commercially sensitive information, making them attractive targets for cyber-attack.[2]

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

The Law Society agrees with the statement in the discussion paper that "Cyber security has always been a shared responsibility".[3] The success of the Government's Cyber Security Strategy requires active engagement from Government and a range of other segments of society, including the private sector. In our view, a closer partnership between the legal profession, Government, financial institutions' fraud squads and law enforcement agencies would assist in the development of minimum standards and clear guidance for safe digital work practices.

3. *Do you think the way these responsibilities are currently allocated is right? What changes should we consider?*

The legal profession plays an essential role in facilitating large volumes of financial transactions which impact the lives of ordinary Australians, such as the sale and purchase of residential and commercial real estate, disposition of assets on divorce and death, and sales and purchase of small businesses. Cybercrime can result in tremendous financial, emotional and legal harms to clients and legal practitioners, and adversely impact the administration of justice. On this basis, responsibility for managing cyber risks should be shared.

Accountability and due diligence should start with the designers and vendors of digital products and services. There are gaps in support for small to medium enterprises ("SMEs"), and we suggest that this could be addressed through greater Government leadership in education, training and the establishment of minimum standards. Small firms and sole practitioners, who may not meet the threshold requirements for mandatory data breach notifications,[4] could be incentivised to sign up for the voluntary scheme if the Government, through the Australian Cyber Security Centre ("ACSC") offered free cyber security audits, training and tools, for example.

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

Government should play a leadership role in ensuring the integrity of the digital economy and our digital society. Potential actions the Government can take in addressing cyber threats are outlined at 1 above.

---

[1] International Bar Association, *Cyber Security Guidelines* (Report, October 2018) 4.
[2] Ibid.
[3] Department of Home Affairs (Cth), Australia's 2020 Cyber Security Strategy – A call for views (Discussion Paper, 5 September 2019) 8.
[4] See *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth).

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

The Government can play a role in supporting consumers' cyber security through taking the actions outlined at 1 above. In addition, the Government should ensure it is simple and accessible for consumers to report instances of cybercrime. Government should consider providing additional assistance to IDCARE to strengthen its efforts to educate consumers about cyber security risks and provide support to individuals who become victims of online crime.

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

Partnerships between the Government and professional bodies, such as the Law Society, help ensure that information on effective cyber strategies reaches those who can benefit from it in a co-ordinated way.

9. *Are there functions the Government currently performs that could be safely devolved to the private sector? What would the effect(s) be?*

As noted above, the Government plays an important role in managing cyber risks in the economy, and this role should continue. Cyber security is central to Australia's economic prosperity and national security; on this basis, Government needs to take a leadership role in ensuring the integrity of the digital economy and our digital society.

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

The Law Society recommends that the current level of funding for the Office of the Australian Information Commissioner be increased to enable this office to effectively carry out its investigative, regulatory, dispute resolution and public education functions, and uphold the rights and protections afforded by the *Freedom of Information Act* (Cth) and the *Privacy Act 1988* (Cth).

14. *How can Australian Governments and private entities build a market of high quality cyber security professionals in Australia?*

Australian Governments and private entities can build a trusted market and a skilled workforce of cyber security professionals by determining requisite qualifications, by setting accreditation procedures, and ensuring ongoing professional development. Dissemination of data breach reports may also assist with the continuing professional development of cyber security professionals and assist in their education regarding diligent investigation processes and best practice.

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

The Law Society agrees that a trusted market of secure products and services and skilled professionals is essential to improve cyber security outcomes in Australia, particularly as could enables the non-government sector to take responsibility for their own cyber security. The availability of affordable cyber insurance providers is one such example of an essential service.

The views of Lawcover have informed our response to this question. The relatively low take-up of cyber insurance in the legal profession likely stems from a lack of awareness as to how this type of insurance operates, protects and benefits legal practice. Lawcover has consulted with its corporate insurance broker Marsh. Marsh advised that, in its view, the main barriers to cyber insurance for legal practices in Australia are lack of awareness and lack of budget. A lack of awareness may relate to the risks, the extent to which risks are covered by existing

insurance policies and the availability of insurance cover. Lawcover concurs with that view, which is why it introduced a foundational level group cyber risk policy for insured law practices at no additional cost in 2018.

Marsh further advised that the cyber insurance market is growing and uptake is increasing. In NSW, a base level of cyber cover is available to legal practices insured by Lawcover, which has acquired a group policy under which its insureds can access cyber experts to assist in the event of a system breach or employee error.

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

The Law Society submits that the Government should adopt a proactive and pre-emptive response to regulating the flow of malicious traffic into Australia by working closely with internet service providers and supporting them to strengthen their cyber security capabilities. In addition, simple campaigns to promote end-user's online safety and best practice around emails could result in consumers more proactively identifying malicious activity themselves.

18. *How can Governments and private entities better proactively identify and remediate cyber risks on essential private networks?*

The role of the ACSC is to lead the Government's operational response to cyber security incidents, organise national cyber security operations and resources, and encourage and receive reporting of cyber security incidents. In fulfilling its leadership function, the ACSC could share more data and critical information with service providers about current and imminent threats. It could also lead a coordinated approach to countrywide attacks.

It would be useful for there to be a single source of reliable information about new and emerging threats for both Government and private sector providers. An example of where this has been done is in Victoria, where the Government has created cyber security infrastructure to develop cyber skills, and commercialise technology research and development, in partnership with the private sector.[5]

22. *To what extent do you agree that a lack of cyber awareness drives poor consumer choices and/or market offerings?*

A lack of cyber awareness and education is likely to drive poor consumer choices and less than satisfactory market offerings. We recommend the following initiatives as a strong starting point to promote cyber awareness:

- Best practice guidelines (particularly targeting SMEs);
- Encouraging appropriate organisations to consider buying cyber insurance; and
- Robust and accessible standards and guidelines.

23. *How can an increased consumer focus on cyber security benefit Australian businesses who create cyber secure products?*

An increased consumer focus on cyber security could incentivise businesses to ensure that security is placed at the forefront of their products or services by design. Security should be the primary consideration, along with privacy in the design and development of products. Interventions that may support this outcome include: a rating system indicating the level of security offered; and a cyber consumer watchdog with the power to bring actions against vendors that misrepresent their product's cyber security profile.

---

[5] Victorian Government, *Cyber Security Strategy 2016-2020* (Report, 2017).

24. *What are examples of best practice behaviour change campaigns or measures? How did they achieve scale and how were they evaluated?*

With regard to international best practice, we note that Singapore's Cyber Security Agency, the national agency overseeing cybersecurity strategy, operation, education, outreach, and ecosystem development, has taken a proactive leadership role in education.[6] We recommend consideration of their initiatives.

2. Offensive Cyber Operations

Beyond the discussion questions, the Law Society would like to make additional observations with regard to OCOs. OCOs can be defined as "operations to manipulate, deny, disrupt, degrade, or destroy targeted computers, information systems or networks".[7] Amongst other means, OCOs are used by the Australian Government to deal with cyber and other threats to national security. OCOs have existed for several years, however broader awareness of their existence has only been realised relatively recently.[8] Rapid developments in technology and the growing sophistication of cyber threats to national security in Australia has correlated with the Australia Government's increased use of OCOs.

The ASD has described the use of the OCOs as a means to "disrupt, degrade or deny our adversaries",[9] emphasising that these OCOs are solely focused offshore. OCOs have the capabilities to go beyond mere reconnaissance and intrusion, as is the case with cyber-espionage, to changing system data or introducing malware into a foreign system. The degree of an OCO invasion and the impact that ensues can vary significantly, from blocking an attempted cyber-attack to proactive hacking.[10]

The Law Society supports initiatives by the Australian Government to respond and adapt to a fast-changing technological environment by developing robust mechanisms that protect against sophisticated cyber threats. OCOs have been regarded as a "cost-effective, non-lethal and flexible method of covertly or overtly exerting power".[11] OCOs can provide a cyber solution to a non-cyber threat, which provides the option to minimise a threat from afar without the need for force or conventional strategies.[12] The Law Society considers it appropriate that the ASD continue to use OCOs not as a law enforcement tool but in response to serious threats to national security from foreign actors offshore, in so far as it is clearly authorised by the *Intelligence Services Act 2001* (Cth) ("the Act").

---

[6] Government of Singapore, *Cyber Security Agency of Singapore* (Web Page) <https://www.csa.gov.sg/>.
[7] Tom Uren, Bart Hogeveen and Fergus Hanson, Australian Strategic Policy Institute, *Defining offensive cyber capabilities* (2018) <https://www.aspi.org.au/report/defining-offensive-cyber-capabilities> ('the ASPI Report'); see, also, William Owens, Kenneth Dam and Herbert Lin, National Research Council, *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (2009), 1, < https://www.nap.edu/catalog/12651/technology-policy-law-and-ethics-regarding-us-acquisition-and-use-of-cyberattack-capabilities>.
[8] Malcolm Turnbull, 'Launch of Australia's Cyber Security Strategy' (Speech delivered at Launch of Australia's Cyber Security Strategy, Sydney, 21 April 2016.
[9] Mike Burgess, 'Offensive cyber and the people who do it'(Speech delivered at the Lowy Institute, Sydney, 27 March 2019).
[10] Max Smeets,'The Strategic Promise of Offensive Cyber Operations' (2018) 12(3) *Strategic Studies Quarterly* 90, 93
[11] Christian Leuprecht, Joseph Szeman and David Skillicorn, 'The Damoclean sword of offensive cyber: Policy uncertainty and collective insecurity' (2019) 40(3) *Contemporary Security Policy* 382, 395.
[12] Eric Rosenbach in Dan Lamothe, Washington Post, *How the Pentagon's cyber offensive against ISIS could shape the future of elite U.S. forces* (16 December 2017) <https://www.washingtonpost.com/news/checkpoint/wp/2017/12/16/how-the-pentagons-cyber-offensive-against-isis-could-shape-the-future-for-elite-u-s-forces/?noredirect=on&utm_term=.fd1c4d5f272c>; Christian Leuprecht, Joseph Szeman and David Skillicorn, 'The Damoclean sword of offensive cyber: Policy uncertainty and collective insecurity' (2019) 40(3) *Contemporary Security Policy* 382, 384.

However, the Law Society notes that such operations can be highly invasive and provocative, present significant risks, and may have implications for civil liberties such as the right to privacy, freedom of association and speech. Therefore, they should not be used lightly. We strongly recommend that OCOs should only be used within the bounds of a clear legal framework and as a proportionate response to significant offshore threats to national security.

It is imperative that the use of OCOs is supported by a clear policy and legal framework to ensure they are not used in circumstances for which they were not intended or authorised to be used. Currently, the legal framework, as set out in the Act, presents some uncertainty as to the scope of OCOs and the circumstances in which their use is authorised. The Act authorises the use of OCOs against foreign offshore actors.[13] However, there is some legal ambiguity as to whether the use of OCOs would be authorised against foreign actors onshore, particularly in the situation where foreign bodies are represented in Australia. Maintaining such a distinction may not be practical or desirable given the degree of global interconnectedness enabled through technology (data storage in foreign jurisdictions through cloud technology being a pertinent example), and given that the threat posed to national security may be significant irrespective of where the source of the threat is located. However, there are other factors that must be balanced, such as the right to privacy, which includes the right not to be subjected to undue state surveillance.

Irrespective of the approach taken, the current scope for interpretation allowed for by the Act has implications for the consistency and legality of OCOs in practice. Under the current legal framework, OCOs could be used against targets onshore without a clear authorisation or warrant process to regulate conduct by the ASD. The Law Society recommends that the 2020 Cyber Security Strategy clarify the Government's position on this; we also recommend that the Act be clarified to reflect this position, ensuring the right balance between protecting national security and the civil liberties of Australians is reached. This would include clear limits being imposed on the use of ASD powers to assist other agencies, including under sections 7 and 11 of the Act.

It is important to note that there is contemporary debate and research suggesting OCOs could constitute an act of war.[14] To address these concerns, more information should be made publicly available, as appropriate, about the approval processes that are undertaken to authorise and carry out an OCO by the ASD. This should include the information that is used by decision-makers to ensure that an OCO is not being used in a way that may constitute an act of war. Information should also be available on the processes to ensure that an OCO is controlled and does not have wider and more harmful impacts which could in turn trigger a greater risk to Australia's national security, as has occurred in other jurisdictions. For example, the NotPetya ransomware attack which spread outside of the intended target and caused $10 billion damage worldwide.[15]

---

[13] *Intelligence Services Act 2001* (Cth) s7(1)(c).

[14] See, eg. Aaron Brecher, 'Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperations' (2012) 111(3) *Michigan Law Review* 423; Lorber (n 9); Benjamin Ramsey, 'An ethical decision-making tool for offensive cyberspace operations' (2018) 32(3) *Air & Space Power Journal* 62.

[15] Christian Leuprecht, Joseph Szeman and David Skillicorn, 'The Damoclean sword of offensive cyber: Policy uncertainty and collective insecurity' (2019) 40(3) *Contemporary Security Policy* 382, 398.

These are important issues and we thank you again for the opportunity to contribute to this consultation. If you have any queries in relation to this submission, please contact Claudia Elvy, Policy Lawyer, on [redacted]

Yours sincerely,

[redacted]

Elizabeth Espinosa
President