The Hon Peter Dutton MP
Minister for Home Affairs
By email: cybersecuritystrategy@homeaffairs.gov.au

28 October 2019

Dear Minister

Australia's 2020 Cyber Security Strategy – contribution from the Cybersecurity and Cybercrime Advisors Network (CyAN)

Thank you for the opportunity to comment on Australia's 2020 Cyber Security Strategy (the 2020 Strategy).

CyAN is an international not-for-profit association (head office in Paris, France) established in 2015. We commenced operations in Australia in 2019, with chapters in both Sydney and Melbourne.

CyAN aims to strengthen cybersecurity and fight against cybercrime through a multi-disciplinary approach based on mutual trust among its members and on complementarity of their profiles and experiences.

Our organisation values diversity, trust and integrity. CyAN's international organisation has made substantial contributions to public policy and practices on issues related to cybersecurity and cybercrime.

Our members contribute to government and societal cybersecurity initiatives through exchanges of good practices, expertise, connections, cooperation and assistance. Many are noted cyber experts in their own right, and the collective experience and insight they bring to our group is impressive.

We commend the Minister and the Department for the open and inclusive manner in which they have sought community input to the new strategy.

CyAN recognises that Australia's 2020 cybersecurity strategy update needs to confront global threats by significantly improving our national and societal cybersecurity capability, and that this strategy will need to be continue to evolve to respond to rapidly changing technology and the associated 'threatscape'.

CyAN aims to be a committed partner to the Australian Government and community in this effort.
There are several elements to the 2020 Strategy that are central to CyAN's objectives that we would like to highlight in our response:

1. We observe that national cybersecurity policies continue to evolve in response to the changing situation with the result that there is increasing sophistication and complexity in regulatory responses. The Parliamentary Library noted in its 2018

Budget Review that the proliferation of Federal Government cybersecurity initiatives has led to a lack of 'explicit detail on how any particular measure ties in with the strategy, or the specific outcomes being sought in cyber policy 'Commonwealth of Australia Department of Parliamentary Services, Budget Review 2018-19, 23rd May 2018, https://parlinfo.aph.gov.au/parlInfo/download/library/prspub/5982057/upload_binary/5982057.pdf: CyAN recommends that the Australian Government implement enhanced measures for the tracking and realisation of benefits from the investments in its cybersecurity initiatives.

2. We believe consideration should be given to reestablishing a separate Cybersecurity portfolio within government. This would send a strong signal to business and the public that the issues our members contend with on a daily basis are receiving the focus and attention they deserve, and underline the economic and social as well as national security aspects of the current threat landscape.

   The Home Affairs portfolio is now very broad, encompassing not only cyber security but also criminal justice, emergency management, immigration and citizenship, multicultural affairs, national security, transport security and settlement services. The observed deficiencies covered in Point 1 above may be better overcome by a narrower portfolio fostering a closer alignment between funding initiatives and key strategic objectives.

3. We commend the Government for its creation of the Joint Cyber Security Centres which promise to build on the partnership between industry and government which began in the early 2000s with the creation of the Trusted Information Sharing Networks which allowed for sectoral collaboration on matters primarily affecting critical infrastructure.

   We see that the cybersecurity threat is global and that international collaboration is required to anticipate and respond to those threats, in a similar manner to international collaboration in healthcare and other sectors of the economy. We note that Australia has been an early adopter of international cybersecurity diplomacy and an advocate of international norms such as the Budapest Convention (2001). CyAN recommends that the Australian Government continues to advocate for multilateral consensus on cybersecurity norms and collaboration against cybercrime.

4. We observe that the Australian Government's initiatives to strengthen the roles of cybersecurity agencies has improved the capabilities of both public and private sector participants to respond to the emerging cybersecurity threats. The establishment of the Australian Signals Directorate as a statutory agency and its merger with the Australian Cyber Security Centre have consolidated and simplified the federal government's capability to respond to cybersecurity threats.

   The creation of AustCyber has started to nurture Australia's indigenous cybersecurity industry and workforce. CyAN recommends that the Australian Government continues to invest in broadening the capability of public and private sector agencies to provide outreach and services to the whole of society, including state and local government agencies, small and medium sized businesses, social and volunteer organisations and the public. The Government needs to consider carefully the balance between increasing compliance obligations and improving incentives for organisations to strengthen their cyber defences.

5. We note that there is a persistent shortage of cybersecurity expertise in the Australian community and in the global market. The lack of basic cybersecurity awareness and skills across the whole of society exposes Australia to a wide range of unsophisticated but pernicious risks that undermine society's trust in its institutions.

   There is also a shortage and lack of diversity in the supply of entry level talent in the cybersecurity profession, exacerbated by the lack of training and career paths available to students and professionals. CyAN recommends that the Australian Government strengthen its focus on basic cybersecurity expertise in the community and on developing a competitive market for training and development of cybersecurity professional expertise

6. We believe that further measures can be taken to promote the adoption of insurance as an element of cyber risk mitigation strategies. There are a number of constraints hindering the growth of the cyber insurance market including a lack of awareness of cyber risk and a lack of clear financial incentives for organisations to invest in insurance. CyAN recommends that the Australian Government strengthen initiatives to educate private sector organisations about the risks and penalties associated with failure to comply with security and privacy legislation.

We would be pleased to consult further with Government in building a strong and effective Cyber Security Strategy.

Yours sincerely

[redacted]

Peter Coroneos
International Vice President
Cybersecurity Advisors Network (CyAN)
Suite 113 Jones Bay Wharf, 26-32 Pirrama Road
Pyrmont NSW 2009 Australia
cyan.network
M: [redacted]