Cybersecurity Coalition

January 2, 2020

Dear Dr. Renwick,

It was a pleasure to meet you in Washington D.C. in November. I was glad to hear that you are in the process of drafting a report on the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* ("the Act") and that you were seeking comment.

Here are some of the views of the Cybersecurity Coalition that I lead on areas where your report could focus:

- As we discussed in our meeting, the Coalition would point you to the Carnegie Endowment for International Peace's paper on encryption entitled *Moving the Encryption Policy Conversation Forward* which has thoughts on areas where solutions can be found and a set of principles for review of solutions. These principles include weighing the proposed solution's utility to law enforcement, assessing the solutions equity to all stakeholders, ensuring specificity to limit abuse or unintended effects, focusing the solution so as not to decrease cybersecurity at large, ensuring that the solution is subject to an authorized legal process, ensuring that the legal standards required for the solutions use limit its scope, and ensuring that the solution and associated processes are auditable, transparent, routinely evaluated, and subject to oversight. We believe that these principles help to ensure legitimacy and consensus among effected stakeholders.

- As you raised in our meeting, the Act's lack of specificity in defining Systemic Weakness and Systemic Vulnerability is a serious concern to both industry and privacy advocates. As it stands, industry is unable to narrow down the extent to which this Act impacts their products and businesses.

  In our view, a systemic vulnerability is any code where a exploit (theoretical or actual) could be utilized to affect more than a single user. The Carnegie report principles outline several areas that can help with this analysis.

  Specifically, the Coalition believes that the Act fails to provide clear assurances that the government will not attempt to weaken encryption in ways that could create substantial ongoing vulnerabilities via other means aside from what might be traditionally viewed as a backdoor such as, unintentionally permitting insecure authentication methods or weakening key

distribution algorithms or systems. Your report could specifically call out these areas and other ongoing systemic vulnerabilities and weaknesses as off limits.

Finally, the Coalition would like clarification that the Act would not require companies to withhold disclosure of the existence of a feature in a product that is included to aid law enforcement Intercept capabilities. Our membership would consider any undocumented or undisclosed legal intercept capability to be a backdoor. As the Australian government has continued to make clear that no backdoors would be required, we would urge you to make clear that companies should not be required to keep secret of any part of the product's functionality.

- The Coalition would like to see an independent process for appeal for organizations to dispute determinations of Systemic Vulnerability and Systemic Weakness. As noted by other organizations and associations, the seriousness of the consequences of complying with the act necessitate a formal independent process by which an organization can challenge the legitimacy of such undefined terms.

- During our conversation at Carnegie, you asked if government should simply demand that the industry find a technical solution. Especially early on in this process, the Coalition is concerned how this would be implemented, as the Carnegie report says, we have not yet found a technical solution that meets the all of the proper balancing tests. Therefore we believe that it will be important for government and industry to work together to find that proper balance in a technical solution.

The Coalition and I appreciate your willingness to engage constructively and seek outside opinion on this vitally important issue. As Australia's conversation around encryption continues to evolve, we would welcome the opportunity to further serve as a resource on both technical and policy questions to ensure encryption is safely deployed and used.

Sincerely,

[redacted]

Ari Schwartz

Coordinator