Lakeba Group
Level 2, 6 The Corso, Manly
NSW 2095, Australia
www.lakeba.com
info@lakeba.com
+61 1300 656 705

27 November 2020
Australian Government
Department of Home Affairs

Dear Department of Home Affairs

Re: The Security Legislation Amendment (Critical Infrastructure) Bill 2020 (the Bill).

Thank you for providing the detailed information and explanatory notes for the proposed amendment to Australia's security legislation as it relates to critical infrastructure. It comes at a time when it is becoming increasingly imperative to protect the essential services Australians rely on across a myriad of sectors. Some of which we took for granted prior to COVID-19.

To this end, Lakeba Group – a venture catalyst – commends the Australian Government in broadening the scope of the bill. Ensuring it has effective safeguards to avoid the risks associated with attacks on our critical infrastructure.

As with all cyber security trends, the risks are always evolving. Requiring continuous assessment of risk avoidance strategies and reliance on the vigilance of stakeholders participating within the network to identify and report cyber-attacks.

Lakeba recommends extending the bill yet further to mitigate the risks entirely. Taking a two-pronged approach of validation and control – as outlined in our previous submission. Approaches that will rely on the Government's commitment to creating a registry and working with industry to develop the appropriate frameworks, regulations, and controls to mitigate risk.

Validation and Control
In the amendment, the Government has laid out plans to develop a register of critical infrastructure assets. While there are several benefits, there is one that will help mitigate cyber security threats – the ability to identify services being used by critical infrastructure assets, such as shared IT (Information Technology) service providers or control systems.

At Lakeba, we commend the increased coverage but believe it needs to go further. To capture all devices that connect into Australia's critical infrastructure.

IoT (Internet of things) devices and sensors are expanding into critical infrastructure at a staggering rate, with the number of IoT devices globally expecting to reach more than 75 billion by 2025. That is over nine IoT devices on average for every person in the world.

With the proliferation of devices and competition in the market, there is a risk that speed to market may be more important than securing these devices to prevent malicious cyber activities from arising. A problem that the industry is already facing – especially in the healthcare sector.

It is therefore vital that any devices operating within Australia's critical infrastructure goes through rigorous testing, certification, and accreditation processes. Recording the outcomes on a register to make it easier for Australia's critical infrastructure owners to select accredited and secure devices to enhance the productivity of their asset without putting Australia and the public at risk.

This could take the form of similar standards such as the Electrical Equipment Safety Scheme in Australia or the Cybersecurity Labelling Scheme in Singapore or ETSI's baseline requirements for IoT devices.

All service providers operating on critical infrastructure networks would need to meet a pre-determined schema of provisions (like ETSI's schema for the implementation of the provisions for the development and manufacturing of consumer IoT). The requirements each provider would need to meet would be commensurate with the criticality of the critical infrastructure data handled or systems it connects with.

Approved testing bodies, consisting of leading industry cyber security entities, would then put these devices through rigorous testing based on the schema requirements. If the device passes these tests, it can then be certified to operate within Australia's critical infrastructure environment.

By creating a standard and register for devices accessing the critical infrastructure network, it will ensure they operate within the security tolerance levels of Australia. Again, Lakeba commends the Government's efforts to collaborate with industry and believes this standard can succeed if we work together to embrace the need to mitigate the risks across the network.

Zero Trust

This is just the start of Australia's journey to developing a mature cyber security landscape. Mitigating the risk of third party devices accessing the network.

However, Australia should continue to enhance its security controls. Taking best practice already taking place in the financial industry to adopt a Zero Trust Model – a model already in use in Australia's latest financial unicorn Judo Bank.

According to the National Institute of Standards and Technology, U.S. Department of Commerce, Zero Trust is the term for an evolving set of cybersecurity paradigms that move defences from static, network-based perimeters to focus on users, assets, and resources.

A zero trust architecture uses zero trust principles to plan industrial and enterprise infrastructure and workflows. Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned). Authentication and authorisation (both subject and device) are discrete functions performed before a session to a critical infrastructure asset is established.

While Australia cannot mandate a Zero Trust approach overnight, all policies should be developed with the approach in mind. Laying the foundations for Australia to begin adopting the technologies and processes required to make it a reality.

No need to recreate the wheel

There is no need for Australia to recreate the wheel when it comes to the development of cyber security policy within critical infrastructure. Governments worldwide – particularly the

European Union and Singapore – have already laid the foundations for successful policy and adoption. And industry is already adopting the most advanced cyber security architecture.

We commend the government in its approach to identifying the solutions to Australia's critical infrastructure security risks in collaboration. Having conceived, created, and commercialised an application vulnerability scan, shield, and runtime supervision technology, our experience has highlighted the need to better protect components in the cloud. These types of technologies, we believe, will be useful to the government during the planning and implementation activities of this bill.

As such, we welcome the opportunity to collaborate or consult in these planning and implementation activities with government and industry.

Some of these activities, but not limited to include:

- Suggestions of the methods of certifying or upgrading the components of critical infrastructure
- Providing a technology framework to facilitate the setting up of cloud-based registry
- Setting up the framework of protecting the critical infrastructure components from attacks

Lakeba will always be happy to lend its support in helping determine the best outcome for government, industry, and the citizens they serve. To this end, we are keen to express our interest in joining the Industry Advisory Committee that has been established to guide Australia's Cyber Security Strategy.

Yours sincerely,

Giuseppe Porcelli,
Chief Executive Officer

Lakeba Group (www.lakeba.com) is a privately held global venture catalyst firm. It accelerates technology ventures which eliminate the frictions caused by analogue transactions across retail, finance, property, and technology. Engaging the intelligence of the masses, the global capacity and distribution of its partners and the proven skill and experience of its team to convert industry needs into commercially successful businesses. Since its launch in 2013, Lakeba Group has conceived, created, and commercialised 13 ventures across its MachineIQ and FinanceIQ portfolios. It has 150 full-time staff across its headquarters in Australia and offices in India, Italy and soon the US.