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

16 September 2020
Australian Government
Department of Home Affairs

Dear Department of Home Affairs

Re: Protecting Critical Infrastructure and Systems of National Significance

Thank you for compiling the comprehensive consultation paper that guides our submission And to the Department of Home Affairs for reviewing our submission.

Lakeba Group, a venture catalyst, commends the Australian Government in committing to protecting the essential services all Australians rely on. It comes at a time when old castle and moat security postures are no longer valid in rapidly decentralised operating environments.

With critical infrastructure being increasingly interconnected and interdependent, connected devices, sensors and applications have proliferated across these networks. Networks that have to allow for the dynamic, decentralised nature of IoT systems that support, augment or update critical infrastructure systems.

According to IT forecaster Gartner, there were already 8.4 billion IoT connections in 2017 and there will be over 20 billion by 2020. Many of which play a central role in power systems, transport, communications, data and cloud, education, food supply chains, health, water and more.

The increasing number of connected devices, sensors and applications creates a threat environment that is both broad and deep. Critical infrastructure providers now have to protect digital sensors, controllers, machines, software and mobile devices from cyber-attacks. To prevent the unauthorised access to the technological infrastructure that powers our nation and society.

Furthermore, while this network of interconnected and interdependent connected devices grows exponentially, critical infrastructure is also leveraging a large third party ecosystem to support its systems. Comprising of a patchwork of manufacturers, service providers, software

providers, components and application developers. And each system is increasingly required to speak to others. Such as human-machine-interface computers with access to remote terminal units, SCADAmaster and programmable logic controllers.

It is vital that Australia addresses this complex environment consisting of the third party ecosystem and consumer endpoint devices that are integral parts of the digital industrial environment.

It is by no means a small task and one that must be tackled with the utmost priority if we are to ensure this increasingly dynamic environment is protected from external threats.

A zero trust approach

Lakeba Group recommends the Government investigates implementing international analyst firm, Forrester's, Zero Trust approach to protecting critical infrastructure.

The zero trust concept centres around the belief that nothing should be automatically trusted whether inside or outside the network. Everything trying to connect to the network, systems or devices must be verified and approved before granting access.

This goes beyond traditional castle-and-moat approach to security. Where static firewalls are placed at choke points to prevent unauthorised access. Proven ineffective as threat actors hid in 'wagons' (external devices entering the network) to breach castle walls and once in, could wreak havoc without much resistance.

The zero trust model looks to address these shortcomings and takes into account the decentralised operating environments of today. It relies on technologies and governance processes to secure an IT environment. Leveraging micro-segmentation and granular perimeter enforcement based on users, location, device, connection and other data to determine who and what to trust.

Zero Trust is already being adopted by the EU and the US. With the U.S. Department of Defence announcing its plan to release a zero-trust framework by the end of 2021. And, Forrester reported that zero trust hit the mainstream in Europe in 2019.

However, while it is recommended Australia follows suit to adopt best-practice cyber security models, zero trust is not a switch you can turn on. And, it's not a policy that is easily retrofitted to current infrastructure. It is a model that requires both a change of thinking and to be developed in the design of new environments.

Standards of Authentication to help plug the gaps
As Australia investigates how it will move forward in its journey to a zero trust model, there is a need to close the gaps during this transition.

Lakeba Group believes there is a need for the development of standards that authenticate APIs, IoT devices and applications for a critical infrastructure context. Much like creating a 'blue tick' of approval for devices, software and applications that operate within critical infrastructure environments. With those approved being able to be more trusted than providers not authenticated against the standard.

While a standard won't guarantee protection from all cyber-attacks, due to the constantly evolving threat landscape, it can provide a high level of minimum protection. Ensuring critical infrastructure, the third party ecosystem that supplies it and consumer endpoints meet requirements to increase the difficulty of penetrating Australia's defences.

The government could look to implement this standard similarly to the Electrical Equipment Safety Scheme, whereby any software, device or application must comply with the standard prior to being able to be embedded in Australia's critical infrastructure or within consumers' homes.

Risk levels could be determined based on what authentication is required within the network. For instance, if a sensor requires access to the SCADAmaster, then it would need to conform to higher requirements compared to an application that requires access to a non-sensitive database.

All authenticated, responsible entities could be registered in a critical infrastructure systems and devices safety registry. This registry could be managed by a peak body composing of cyber security experts, including penetration and vulnerability testers, OWASP, reverse engineering experts, networking specialists and other cyber security bodies.

In creating this peak body, a comprehensive standard can be developed and managed. API connections, IoT and mobile devices, and applications operating within the critical infrastructure can then be authenticated against this standard on a yearly basis. Thus implementing a high minimum security standard within critical infrastructure, while enabling Australia to better transition to a zero trust model.

Securing the third party ecosystem is critical if Australia is to ensure control systems, devices and sensors are appropriately secured and authorised to access our critical infrastructure. It will provide Australia with a registry of all entities that participate in this ecosystem and how they may impact the security of critical systems.

Standards will be set and met by ecosystem members to ensure they build security into any and all solutions that could potentially comprise critical infrastructure operating systems. It means only authorised and more trusted entities could gain access to critical devices and communicate within the network, leveraging principles of segmentation and least privilege access.

Why a standard is needed

While security is a concern for many businesses providing software and devices into the Australian critical infrastructure ecosystem, it does not mean they operate with Australia's interests in mind.

One such example is Australia's emerging renewable energy market – an increasingly important player in Australia's energy mix. Solar power is decentralising the energy market, enabling Australia's to purchase their own panels to generate their own electricity and connect excess into the grid.

The problem, however, is that there isn't an overarching standard on what systems they can buy and install. There are no obvious approved suppliers. This often leads to Australians choosing suppliers based on price, rather than taking into account any security or safety implications, particularly ones that place Australia's national security at risk.

This has led to some consumers choosing solar panels and inverters that are sequestering data off of Australian shores. While one person's solar usage may seem harmless, when you have the data of a large community, international threat actors could have access to critical information. Such as surges of energy usage, what it is being used for or even gain the ability to reverse engineer the software to manipulate the devices and access the energy network.

As we continue to see increased devices connecting to our critical infrastructure, it is vital Australia ensures the highest possible security standards are met. Standards which Australian critical infrastructure providers, its third party ecosystem and even consumer devices must meet.

Enhancing Australia's cyber capabilities

By creating a peak body and standards for the third party ecosystem, it will ensure it operates within security tolerance levels of Australia. It can be achieved by public-private partnerships that focus on leveraging each party's expertise. Allowing for specialisations and niche skills to be utilised in the authentication of the ecosystem.

It will also create a market for certification and audits that will further enhance the cyber capabilities of Australia's workforce. Ensuring cyber security is at the forefront of compliance and risk requirements for businesses wanting to operate within Australia's critical infrastructure.

This will require the training of cyber security staff on zero trust models and the ability to test and authenticate devices and software. New jobs and businesses could be created as an audit industry is created around the critical infrastructure ecosystem.

Overall, creating a new standard for devices, software and applications that participate in Australia's critical infrastructure ecosystem, will only be of benefit to Australia. While it may be perceived as a further requirement for business, it is as necessary as Electrical Equipment Safety Scheme to protect Australia's national interests and society.

Lakeba Group would welcome any discussion around the potential of creating a standard for API, device and applications operating in Australia's critical infrastructure environment. And believes this will be vital in protecting Australians from serious data breaches moving forwards.

Yours sincerely,

Giuseppe Porcelli
Chief Executive Officer

About Lakeba Group
Lakeba Group is an Asia Pacific high-growth company, recognised by London's Financial Times.

We have 160 employees based in Australia, India, Italy, the UK and the US. Supporting over 1,000 business customers performing more than 68,000 transactions on our platforms.

A venture catalyst, Lakeba Group uses the intelligence of the masses, the genius of our partners, the skills of our staff and the experience of our investors. To eliminate the frictions hindering the masses.

Turning digital technologies into ventures. With the skills, services and frameworks to replicate success.

Lakeba currently has six ventures commercialised across its FinanceIQ and MachineIQ portfolios, with seven in its R&D lab LakebaTomorrow,