April 2023

RE: 2023-2030 Australian Cyber Security Strategy Discussion Paper

The Honorable Clare O'Neil
Minister for Home Affairs and Minister for Cyber Security

BlackBerry commends the Department of Home Affairs, and in particular the Minister for Home Affairs and Cyber Security, for her leadership in developing a National Cyber Security Strategy. BlackBerry is grateful for the opportunity to provide input into this important endeavour as Australia strives to become the most cybersecure country in the world by 2030.

BlackBerry is a world leader in cyber security. For close to 40 years, BlackBerry has invented and built trusted security solutions to give people, governments and business the ability to stay secure and productive. Today, our software is used to protect 17 of the G20 governments and secures more than 500 million endpoints. Our customers include 45 of the *Fortune 100* companies, 9 of the 10 largest banks, 9 of the 10 largest automakers, 24 of the top 25 global electric vehicle automakers, and 8 of the top 10 medical device manufacturers, to name a few.

As Australia invests in its digital future, cyber security will be key to fostering innovation and securing trust in our data-driven world. As Minister O'Neil highlighted in the wake of the combined breaches of Optus, Medibank and Latitude, "there probably is not an Australian who either has not been impacted personally [by cyber attacks] or does not have a close family member that has." (The Mandarin, April 4, 2023)

In a context where essential services, critical infrastructure, national security and the daily function of every Australian relies heavily on digital infrastructure, keeping up with the challenges presented by the digital age is imperative. BlackBerry believes that Australia's National Cyber Security Strategy is an essential component of this endeavour, particularly in a heightened geopolitical context where everything and everyone is connected to the Internet, and urges the department of Home Affairs to consider incorporating the following recommendations into the National Cyber Security Strategy as foundational elements:

1. Prioritize the cyber security of Small and Medium Sized Enterprises (SMEs) – the backbone of Australia's economy

The majority (99%) of businesses in Australia are Small and Medium Sized Enterprises (SMEs). SME's contribute more than half of Australia's economic activity and employ 66 percent of Australian workers.[1] SMEs represent the backbone of Australia's economy, and need to be protected from increasingly sophisticated and devastating cyberattacks.

While organizations across every industry sector run the risk of a cyber breach, few carry the same real-world risk from cyberattacks as SMEs. The following statistics highlight why more needs to be done to help Australia's SMEs improve their cyber defences:

- SMEs face an average of 11 cyber threats per device, per day (BlackBerry 2022 Threat Report)

[1] Australian Small Business and Family Enterprise Ombudsman: https://www.asbfeo.gov.au/contribution-australian-business-numbers

- The average cost of a cyber breach is US $2.4 million (Forrester[2])
- Only 14 per cent of businesses have cyber insurance coverage limits above $600,000 (BlackBerry Cyber Insurance Study)
- 59 per cent of businesses hope that the government will cover damages for attacks linked to nation-states (BlackBerry Cyber Insurance Study)
- Cyberattacks are devastating to SMEs. 60 percent of SMEs that fall victim to a cyberattack are out of business within six months (BlackBerry 2022 Threat Report)

Faced with a global cybersecurity skills shortage of more than 4 million, the gap between those who are protected from cyberattacks and those who cannot afford to be protected only grows. As Minister O'Neil recently underscored, we need to "shift cyber risks away from our most vulnerable members towards those who are best placed to manage it, including software and cyber service providers." (ITNews, March 23, 2023).

BlackBerry strongly advocates for the National Cyber Security Strategy to prioritize measures to help SMEs enhance their ability to prevent cyber threats from impacting their businesses by providing SMEs with incentives, funding and cyber defence grants so that they can acquire advanced, AI-driven, cyber security tools, invest in cyber talent, and access external cyber security experts to reduce their exposure to cyber risk proactively. In a context where it is extremely difficult for SMEs to hire and retain cyber talent, the use of AI-driven cybersecurity solutions that can prevent cyber attacks and automate responses will become ever more important. Australia should consider supporting and promoting such solutions as a baseline to elevate Australia's cyber resilience. Doing so will help SMEs focus their scarce people resources on challenges and opportunities that need the most attention. Ensuring that all Australian businesses have the ability to access the most advanced AI-driven cyber solutions is particularly important in a context where malicious actors are increasingly leveraging automation tools (ChatGPT and other adversarial AI) to reach 'bigger fish'. Whether it is for political disruption or financial gain, threat actors will continue to target critical infrastructure and manufacturing by targeting small businesses along the IT supply chain.

2. Adopt a prevention-first approach to Australia's cyber security

Protecting Australians from cyber threats requires more than incident response – it is nothing less than a whole-of-society endeavor to prevent attacks before they happen. With the pace of digitalization accelerating globally – especially since the start of the pandemic – the Australian government simply cannot afford to leave its businesses, infrastructure and communities continually exposed to cyber threats. To that end, BlackBerry recommends that Australia's National Cyber Security Strategy recognize the imperative of adopting a prevention-first approach to cyber security, in addition to its investments in incident response and threat hunting.

A prevention-first approach involves the adoption of advanced AI-driven cybersecurity solutions that are designed to prevent cyber threats and protect systems *before* they fall victim to cyberattacks. If malware cannot execute on software used by businesses, critical infrastructure operators, governments and other organizations, then the downstream consequences, and the resulting efforts to trace, contain, and remediate the damage, are dramatically reduced. This approach proactively protects organizations and reduces the administrative burden on security operations center staff who are often besieged by alerts and incidents. In a context where adversaries are increasing in sophistication, advanced AI-driven

[2] Forrester, Breaches by the Numbers: https://www.forrester.com/blogs/breaches-by-the-numbers-adapting-to-regional-challenges-is-imperative/

approaches to cyber security can play a significant role in proactively securing critical infrastructure and automating responses to continuously defend Australians against complex cyber risks.

It is critical that Australia continue to shift its approach from a reactive to a proactive stance. We commend the Australian government for recent measures taken to strengthen its cyber defences, including efforts to disrupt online criminal gangs, issue new penalties for data privacy and establish a stronger line of defence with incident response. However, we believe that the Australian government can do more to get in front of the attackers with a prevention-first approach.

As Minister O'Neill has repeatedly noted, a focus on incident response inevitably forces Australians to deal with the after-effects of a cyber attacks. To get ahead of the attackers we must focus on prevention. This is the most prudent and cost-effective approach. A prevention-first approach can be realized by standardizing the adoption of advanced AI-driven cyber security tools that have the demonstrated capability, based on proven industry-metrics (i.e., tested on billions of files; examined millions of file characteristics, good and bad) to block malware before it executes on the endpoint. Adopting an advanced AI-driven, prevention-first, approach to cyber security as a national standard would help position Australia as the most cyber secure country in the world by 2030.

The deployment of AI-driven, prevention-first, cyber security solutions and services is particularly important for businesses and critical infrastructure. The software used by businesses and critical infrastructure entities involves a complex web of dependencies with numerous third-party developers and components. In many cases, these systems are dependent on legacy technologies that are outdated and vulnerable to cyber attack. With experts indicating that more than 90 percent of commercial applications contain outdated or abandoned open source components, the case for incentivising critical infrastructure operators and businesses to adopt a prevention-first approach to cyber security that leverages advanced AI-driven cybersecurity solutions couldn't be more clear. Doing so will help proactively protect Australians and the services they depend on from increasingly sophisticated cyber threats before they compromise these systems.

3. Help critical infrastructure owners and operators, including manufacturing, prioritizes cybersecurity investments to prevent their Operational Technology (OT) from being compromised by cyber attacks and implement a 'secure by design' / 'secure by default' approach to cyber security

We commend recent announcements and measures taken by the Australian government to strengthen the security of critical infrastructure, including in adopting the *Security of Critical Infrastructure Act of 2018* and the more recent publication of *Principles and Approaches for Security-by-Design and Default* jointly with Five Eyes Nations. Ensuring that these principles and regulations are implemented across the board by Critical Infrastructure entities is essential.

Historically, OT systems were air-gapped and physically isolated from IT networks. Today, more OT systems are being connected to IT networks to take advantage of the benefits of digital technologies including optimization, sustainability, operational performance, asset management and reduced cost. These initiatives, while critical to the future of Australia, are also increasing the potential attack surface available to bad actors to exploit. OT systems are often decades old and rely on outdated software that is no longer supported. According to IDC, there will be over 49 billion connected IoT devices in place by 2026. The ongoing march toward Industry 4.0 and digital transformation is exposing vulnerabilities in many critical applications across the medical, manufacturing, electric, mining, oil and gas sectors to mention a few. The scale of these vulnerabilities and the cyber attack surface will only grow as "Smart Cities", "Smart Manufacturing" and "Smart Industrial Control Systems and Infrastructure" come online.

The government and industry must prepare for the physical and digital collide that is happening and escalating across our infrastructure and all industry sectors. As the Hon Ed Husic MP noted recently when announcing the $15 billion National Reconstruction Fund bill, "the most successful modern economies are built on strong, ***secure***, advanced manufacturing capabilities" (*emphasis added*). Australia's National Cyber Security Strategy should work to ensure that Australia's OT infrastructure, particularly in the manufacturing sector, is secure from cyber attacks.

A recent BlackBerry commissioned survey of Australia's manufacturing sector indicated that 79 percent of respondents had been subject to a cyber attack in the past 12 months. In addition, 87 percent of respondents in Australia admitted their manufacturing functions are running on outdated and unsupported legacy operating systems. Cyber security breaches can result in financial losses, factory shut-downs, compromising personnel safety, and IP theft. The development of a short and long-term strategy that ensures a forward-thinking view of how to secure OT used in Australia's manufacturing sector should be a fundamental element of the National Cybersecurity Strategy, in tandem with the implementation of the National Reconstruction Fund**.**

To that end, BlackBerry urges the Australian government to encourage end-to-end risk management reviews and the adoption of proactive security practices in OT environments. This could include:

A) A broad-based cybersecurity review of legacy IT (software and hardware) used in critical infrastructure with a cataloguing of potential vulnerabilities;

B) Incentivizing investment in advanced AI-driven cyber security products and measures that proactively prevent malware from infecting these OT systems and immediately identify and patch vulnerabilities; and

C) Helping manufacturing industries to equip their staff with cyber security skills, and where necessary augment protections with external security teams to help orchestrate security actions that prevent, detect, stop and remediate cyber incidents.

4. Improve public-private collaborations to promote cyber resilience and secure access to the digital economy.

Experience in allied countries has shown that it is impossible to protect residents from growing cyberattacks without institutionalized knowledge-sharing and collaboration between the public and private sectors from the strategic to tactical levels. As part of the National Cyber Security Strategy, Australia should give high priority to the building of a close working relationship with the private sector, one that integrates private sector expertise into its national security planning and response.

To that end, BlackBerry would urge the Australian government to improve cyber threat intelligence and knowledge-sharing and pro-active cyber security collaboration between government and industry. Such a platform would enable industry and government to exchange threat intelligence, work proactively to plan for cyber attacks, and jointly test and deploy innovative cybersecurity solutions. In a context of evolving cyber threats, compounded by a cyber talent shortage, the sharing of real-time, high quality cyber threat information is essential. This can be done by establishing **an Australian Cybersecurity Collaborative** that is mandated to bring together private and public sector actors to proactively plan and respond to cybersecurity related threats and incidents.

In 2021, the US Congress authorized the creation of the Joint Cybersecurity Defense Collaborative. This entity, housed within the Cybersecurity and Infrastructure Security Agency, is mandated to lead collaborative, public-private sector cyber defense planning, cybersecurity information fusion, and the purposeful dissemination of cyber defense guidance to reduce cyber risk to and increase the resilience of National Critical Functions in the United States. This entity has proven effective, particularly in the wake of the crisis in Ukraine in enhancing information sharing and public-private collaboration on cybersecurity in the US, and could be a model for Australia to follow.

Of particular importance, would be for Australia to take a leadership role, in collaboration with Five Eyes nations and AUKUS, to work closely with Pacific nations in their fight against cyber attacks. The Australian Government has emphasized the importance of listening to the technological needs of Pacific Island states and helping to build resilience across the region. It is essential that the government act on that intent by collaborating with industry and through proactive threat intelligence sharing and cybersecurity preparedness planning platforms and mechanisms.

5. Conclusion

BlackBerry is aligned with the Prime Minister's statement – that cybersecurity is Australia's national security. However cybercrime is borderless, making it a shared national security challenge.

Protecting Australia cannot be done in isolation. Effective cyber security demands true international and private/public sector collaboration that will help to defend the citizens, industry and government of Australia – in partnership with partner nations.

We have offered our advanced AI-driven solutions and expertise in embedded systems, mission critical software and expertise in secure communications to support governments and industry across the world. BlackBerry extends the same support to the Government and citizens of Australia.

BlackBerry appreciates the opportunity to provide input into this important Cyber Security Strategy and thanks the Australian government for considering our input.

Sincerely,

John de Boer
Senior Director, Government Affairs and Public Policy
BlackBerry Limited