Cybersecurity Coalition

April 14, 2023

RE: 2023 – 2030 Australian Cybersecurity Strategy Discussion Paper

The Cybersecurity Coalition ("the Coalition") submits the following comments in response to the public consultation issued by the Expert Advisory Group on the 2023-2030 Australian Cybersecurity Strategy. The Coalition appreciates the Australian Government's openness in engaging industry on this important topic and looks forward to working with the Government to ensure best cybersecurity practices are implemented in the National Cyber Strategy. The Coalition further commends the Government for having the goal of becoming the most cyber secure nation by 2030.

The Coalition is composed of leading companies with a specialty in cybersecurity products and services. We are dedicated to finding and advancing consensus policy solutions that promote the development and adoption of cybersecurity technologies. We seek to ensure a robust marketplace that will encourage companies of all sizes to take steps to improve their cybersecurity risk management.

The Coalition has worked with more than 20 governments around the world on the development of national cybersecurity policies, many of which were designed to address issues that are raised in the paper. Having just working closely with the US Government on their National Cyber Strategy, we are acutely aware of the need to effectively address the challenges that you identify, as well as the difficulty of doing so in an effective manner.

We provide the following responses to the questions with a view to advancing our shared objective of safeguarding and ensuring resilient critical infrastructure as well as having international harmonization and regulatory alignment. As the conversation around becoming the most cyber secure nation in Australia continues to evolve, we would welcome the opportunity to further serve as a resource to ensure the success in achieving the Government's objectives.

Respectfully Submitted,

The Cybersecurity Coalition

CC:

Ari Schwartz, Venable LLP
Alexander Botting, Venable LLP
Tanvi Chopra, Venable LLP

Response to Discussion Questions

Q1: What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?

With the proliferation of threats attacking critical entities and the increasing dependence on ICT, there is a demand for a more intentional, more coordinated, and a better-resourced approach to cyber defense. To address this, the Strategy can focus on implementing effective threat information sharing among public and private sectors, ensure the development of a diverse and robust national cyber workforce, and focus on replacing legacy systems with more secure technology.

These are all areas that other governments who have recently released their National Cyber Strategies are focused on. However, there is a key piece that can further help Australia become the most cyber secure nation as well as the most informed nation, and that is by pushing for international harmonization. Given the lack of regulatory alignment around global cybersecurity, we'd like to see the Australian Government to be a global leader to mitigate divergence and further regulatory cooperation on cybersecurity. This strategy can help stand up a global forum to work on areas of mutual cyber policymaking to drive alignment, enhance cybersecurity outcomes, and avoid imposing unnecessary regulatory burdens on stakeholders.

Q2: What legislative or regulatory reforms should Government pursue to: enhance cyber resilience across the digital economy?

There are a number of legislative and regulatory reforms the Government can implement to enhance cyber resilience and support national security and public safety. Specifically, the Government should develop clear baseline cybersecurity requirements for critical infrastructure entities to reduce risk and ensure their networks are secured.

While a largely voluntary approach to critical infrastructure cybersecurity has led to some global improvements, a general lack of mandatory requirements has too often resulted in inconsistent and insufficient protections against cyber intrusions. Attacks against critical infrastructure companies are posing serious problems, from service disruption to physical threat to human lives. When the consequences of disruption or breach affect large portions of the population, having a voluntary approach is insufficient. As a result, regulations to establish cybersecurity responsibilities for systemically important entities should be implemented.

In addition, the Government should communicate clear guidance to non-critical entities regarding voluntary steps they can take to enhance resilience and better protect themselves against cyber threats.

Q2c: Should the obligations of company directors specifically address cyber security risks and consequences?

Yes. Given the alarming number of cyber-attacks against the private sector that lead to significant business disruption, potential consumer harm, and reputational risk, ensuring the

adequacy of a company's cybersecurity should be under the purview of the Board of Directors' responsibilities. At a minimum, boards should have a clear understanding of who at their company has responsibilities for cybersecurity risk oversight. Boards should be proactively taking steps to confront any cyber risks and the resulting fallout from incidents.

Last year, the U.S. Securities and Exchange Commission (SEC) proposed a rule targeting this issue, signaling the importance of effective corporate governance. If finalized, this rule would require mandatory disclosures regarding companies' board of directors' oversight of cybersecurity risk, as well as individual board members' cybersecurity expertise. We recommend Australia to take a similar approach and ensure directors are obligated to appropriately address cyber risks.

Q2f. Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals by: (a) victims of cybercrime; and/or (b) insurers? If so, under what circumstances? i. What impact would a strict prohibition of payment of ransoms and extortion demands by cyber criminals have on victims of cybercrime, companies and insurers?

Many governments have taken a stance of prohibiting ransomware payments to cyber criminals by both organizations victimized by ransomware attacks and more broadly financial institutions, cyber insurance firms, and incident response firms. In particular, the Office of Foreign Assets and Controls (OFAC) of the U.S. Department of Treasury issued an advisory highlighting that organizations that make payments are not only encouraging future payments but also may risk violating OFAC regulations. Under OFAC, it is illegal to facilitate the payment to individuals, organizations, regimes, and certain countries that are on the sanctions list.

While many organizations pay ransoms with the belief that their data may be recovered, that is almost never the case. We encourage Australia to also discourage organizations from paying ransoms because there is never a guarantee that stolen data will not be exploited again for further payments.

Q2g. Should Government clarify its position with respect to payment or nonpayment of ransoms by companies, and the circumstances in which this may constitute a breach of Australian law?

Yes, we encourage the Government to clarify that making payments may constitute a breach of Australian law.

Q3. How can Australia, working with our neighbors, build our regional cyber resilience and better respond to cyber incidents?

The Australian Government can best work with its neighbors and allies to better respond to cyber incidents through effective forums that encourage information sharing at a government-to-government level about potential approaches and best practices. For example, with Australia leading the International Counter Ransomware Taskforce, the Government is well-positioned to exchange cyber threat intelligence with other countries to increase early warning capabilities and prevent attacks.

Q7: What can government do to improve information sharing with industry on cyber threats?

Similar to how the Government benefits from awareness and visibility into cybersecurity risks by companies, companies can benefit from resources and notifications of potential threats. Threat intelligence sharing should be a two-way process and the Government should identify ways to make information sharing more effective through the implementation of best practices such as:

- Keeping information sharing voluntary, thereby allowing companies to share information they deem relevant;
- Providing legal protections for any information shared; and
- Keeping a separation between agencies that are tasked with support and threat intelligence aggregation, and those tasked with regulatory oversight

Q9: Would expanding the existing regime for notification of cyber security incidents (e.g. to require mandatory reporting of ransomware or extortion demands) improve the public understanding of the nature and scale of ransomware and extortion as a cybercrime type?

Generally speaking, requiring mandatory reporting of ransomware will accelerate the gravity of the situation once an entity is required to notify a government agency of a particular incident. By alerting authorities, it can support the public good by providing details that can help defend against future attacks and prosecute cyber syndicates.

Q12: What more can Government do to support Australia's cyber security workforce through education, immigration, and accreditation?

Cyber workforce development is a global challenge, and it must be a global solution. Australia can play its part through the following ways:

- *Education:* The Government can work with academia by introducing cyber education at a young age and incorporating cybersecurity in curricula for undergraduate and graduate degrees.

- *Immigration:* The Government can help with investments to increase student participation through grant incentives and immigration policies that attract new talent.

- *Accreditation:* The Government can expand access to non-traditional pathways, such as through cybersecurity certificates.

We encourage the Government to work with academia and the private sector to identify and address cybersecurity workforce needs, and to collaborate to raise cyber education broadly across society. We are confident that investing in these two areas will not only benefit Australia with stronger cyber posture, but the rest of the globe as well.

Q13: How should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians? a. Should government

consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?

Having harmonized requirements and a single reporting portal for cyber incidents would lessen the burden for companies when experiencing an attack. Agencies that often have conflicting timelines or different reporting requirements add an unnecessary layer of complexity to the incident reporting and response processes.

In a context where affected entities are rushing to contain a serious cybersecurity incident, adding contradictory reporting requirements to different agencies makes strenuous situations even more so. We recommend that the Government creates a way for companies to report only to one entity rather than different regulators.