April 15, 2023

Andrew Penn AO
Chair of the Strategy Expert Advisory Board
Department of Home Affairs
Via Email: auscyberstrategy@homeaffairs.gov.au

Re: Discussion Paper for 2023-2030 Australian Cyber Security Strategy

Dear Mr. Penn,

Tenable®, Inc. (Tenable) appreciates the opportunity to provide input to the 2023-2030 Australia Cyber Security Strategy, and we are grateful for the chance to engage in the ongoing development of Australia's cyber security efforts. In this response, we endeavour to address questions included in the discussion paper and provide some additional observations and considerations.

Tenable is the Cyber Exposure Management company. Headquartered in Columbia, Maryland, we maintain a presence in more than 80 countries with more than 1,900 employees globally. Approximately 40,000 organisations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable has extended its expertise in vulnerability management to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers now include approximately 60 percent of the Fortune 500, approximately 40 percent of the Global 2000, and large government agencies. In Australia, Tenable's customers include more than 62 government departments and agencies and Tenable could be viewed as the default vulnerability management solution across the Federal Government.

Tenable provides organisations with an unmatched breadth of visibility and depth of analytics to measure and communicate cyber risk. We believe cyber security is foundational to making better and more strategic decisions. Our goal is to eliminate blind spots and help organisations prioritise which actions they can take to most efficiently reduce exposure and loss. Simply put, Tenable empowers organisations of all sizes to understand and reduce their cyber risk.

Over the past few years, we have noted a dramatic increase in the frequency of successful cyber attacks, including ransomware, against Australian operators of critical infrastructure. New ransomware and extortion groups routinely exploit known vulnerabilities to gain access into organisations, with at least 31 new groups discovered from November 2021 to October 2022. This has resulted in intensified ransomware attacks accounting for more than 35 percent of data

breaches.[1] The Optus and Medibank breaches late last year were among the largest cyber attacks in the nation's history and resulted in millions of personal data potentially being exposed to identity theft and fraud. Tenable supports Australia's efforts to develop a forward-looking strategy that improves cyber security resilience across the country.

Government policy should not allow for "learned helplessness" by federal government departments and agencies or private industry. Helplessness allows individuals and organisations to remain negligent and avoid accountability for not taking even the most basic steps to improve cyber posture. While the government can certainly play a stronger role in deterrence, attributing cyber attacks, and establishing sanctions regimes, those efforts should not replace the promotion and implementation of basic cyber hygiene practices and processes.

The appointment of a new national Coordinator for Cyber Security and creation of a National Office for Cyber Security within the Department of Home Affairs are important foundational steps to streamline Australia's cyber security capabilities and policies.

Detailed below are Tenable's responses to specific questions within the Department's discussion paper.

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

Tenable believes that achieving an ambitious goal such as this requires a multi-pronged strategy that incorporates best practices in multiple areas of cyber security and leverages the full breadth of the resources available to Australia and its government. Specifically, we recommend that the following three ideas be included in any cyber security strategy that Australia ultimately develops:

1. Establish baseline cyber security requirements or standards of care for critical infrastructure that align with international standards. Australia should require owners and operators of critical infrastructure organisations to implement risk-based, flexible, outcomes-focused, baseline cyber security requirements, which are aligned with international, consensus-driven standards and other best practices. The recent cyber reforms for critical infrastructure operators in Australia, which require providers to adopt a risk-management framework, such as the ISO 27001 standard, the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), the Australia Essential 8 standard, or a commensurate cyber security standard, are a positive step

[1] Tenable, "2022 Threat Landscape Report," https://static.tenable.com/marketing/research-reports/Research-Report-2022_Threat_Landscape_Report.pdf

forward[2]. In the U.S., the Cybersecurity and Infrastructure Security Agency (CISA) recently issued cross-sector cyber security performance goals (CPGs) based on the NIST CSF. While the CPGs are voluntary, they offer a helpful baseline for critical infrastructure organisations, allowing them to prioritise cyber security actions that are most useful in addressing cyber risk. Basic cyber hygiene for critical infrastructure operators includes continuous understanding of what assets are on networks, ensuring effective identity and access management processes and practices, scanning for and patching known vulnerabilities, and implementing incident detection and response capabilities.

2. Support and strengthen value added engagement between the private sector and public sector. Partnerships between the public and private sectors that foster information sharing are essential to protecting critical infrastructure and furthering cyber security. The Australian government should consider establishing a mechanism similar to CISA's Joint Cyber Defense Collaborative (JCDC), of which Tenable is a partner. The JCDC brings together representatives from private industry and key government agencies to drive strategic planning and incident response capabilities. This type of operational government-industry engagement has been a positive step forward.

3. Secure IT and OT systems and their convergence, which has become a national security imperative. Public-private sector collaboration to address cyber threats is essential to building resilient and robust converged information technology (IT) / operational technology (OT) environments. The combination of IT and OT systems makes OT systems susceptible to the same risks of malware and threats that IT systems face today. Organisations often lack visibility into their OT environments, which is exacerbated by the traditional silos within which OT and IT personnel operate. The Australian government should take steps to clearly understand the vast and interconnected nature of their OT devices and infrastructure. This would allow them to then make risk-informed decisions about how to prioritise their cyber security budgets to best protect the most consequential of those assets.

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

We applaud the Australian government's efforts to increase the nation's cyber resiliency. Recent cyber reforms, requiring critical infrastructure providers to adopt cyber risk-management frameworks, such as the ISO 27001 standard, the NIST CSF, the Australia Essential 8, or other commensurate security standards is an important step forward towards enhancing cyber resilience across the digital economy[3]. The government should ensure that these policies allow for

[2] Amendments to the Security of Critical Infrastructure Act 2018. https://www.legislation.gov.au/Details/C2022C00160
[3] Ibid 2.

continued flexibility and innovation in cyber practices and processes. Enhancing and harmonising regulatory frameworks will be critical to achieving effective outcomes.

The Australian government can also ensure that cyber security practices for federal departments and agencies serve as a model for the broader ecosystem. Continuous assessment is a key practice that the Australian government should implement to protect its systems and to model best practices for industry. Protecting Australia's cyber security requires maintaining a real-time, continuous inventory of all IT and OT devices, software, systems, and assets within their areas of responsibility, including an understanding of any interconnectivity to other systems.

We recommend that the Australian government reinforce the need for federal departments and agencies to gain visibility into mission-critical environments so it can understand the scale of cyber security challenges and begin to systematically address the serious risk. Achieving this visibility is a significant step forward for federal departments and agencies to protect their critical IT and OT assets against evolving cyber threats. Tenable further recommends the Australian government explore a requirement for federal agencies to have comprehensive visibility into assets and vulnerabilities across their organisation. This includes external unknowns, cloud workload and resources, operational technology, network infrastructure and endpoints, web application, and identity systems. Without this requirement, the government's digital systems will lack adequate visibility into their cyber exposure.

2(c). Should the obligations of company directors specifically address cyber security risks and consequences?

This question speaks to a major problem currently impacting corporations: the lack of ownership of and responsibility for cyber security measures within leadership. At its heart, a cyber breach or threat is not just a technical problem; it represents potential damage to a company's reputation, finances, and future success. In addition to the costs of remediation from a cyber attack and loss of customers, revenue, and reputation, there are risks of shareholder lawsuits, customer lawsuits, increases in insurance premiums, and increased scrutiny from external auditors and the board of directors. There are indirect consequences to cyber failures, as well. Cyber attacks can distract management, resulting in new problems; they can also trigger customer audits of a company's cyber security defences, which can lead to the involvement of outside counsel and other third parties, plus significant added expenses. Forcing corporate leadership to pay attention to this can serve as a significant driver for companies to establish baseline cyber security practices and processes.

The Australian government should implement a rule that requires all public companies to disclose that they have adopted appropriate cyber risk management frameworks to address their cyber security risks. As an example, the U.S. Securities and Exchange Commission (SEC) has shared a Proposed Rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

that would require public companies to disclose their policies and procedures for identifying and managing cyber security risks, management's role in implementing cyber security policies and procedures, and the board of directors' cyber security expertise.[4] Requiring greater transparency of cyber risk practices and oversight forces companies to treat cyber security risk as a business risk and will lead to stronger cyber security governance and accountability among corporate leaders and boards.

7. What can government do to improve information sharing with industry on cyber threats?

The Australian government has an opportunity to greatly improve information sharing by breaking down the traditional siloed approach to cyber security and incident response. Tenable recommends implementing standardised, technology-neutral, real-time, interoperable information sharing mechanisms to promote the sharing of sensitive information across agencies. Cyber attacks often target multiple critical infrastructure sectors, and attackers can move at machine speed to compromise multiple industrial sectors. Cyber defences need to match this threat, and it is imperative for critical infrastructure sectors to securely communicate with each other to get the right information to the right person at the right time and in a standardised, technology-neutral way to leverage cyber threat and vulnerability information from the broader critical infrastructure ecosystem.

In the United States, CISA established the JCDC to lead "integrated public-private sector cyber defence planning, cyber security information fusion, and dissemination of cyber defence guidance to reduce risk to critical infrastructure and National Critical Functions."[5] Tenable is a proud Alliance Partner of the JCDC, which has enabled us to collaborate with CISA across a range of cyber security issues and challenges, as well as to provide strategic insights and operational response acumen. Managing vulnerabilities is essential to secure critical IT and OT infrastructure, and the work done by JCDC and CISA promotes the prioritisation of network security. In fact, known vulnerabilities dating as far back as 2017 were so prominent in Tenable's 2022 Threat Assessment Report findings that they occupied the top spot in the 2022 list of the top 5 vulnerabilities[6].

13. How should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians? Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?

---

[4] SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies, https://www.sec.gov/news/press-release/2022-39.

[5] U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, "Joint Cyber Defense Collaborative," https://www.cisa.gov/sites/default/files/publications/JCDC_Fact_Sheet_508C.pdf.

[6] Ibid 1.

Tenable applauds the Australian government's efforts to pursue additional means of responding to cyber incidents above and beyond its current cyber measures. We agree that harmonising existing requirements for reporting will improve the nation's cyber resilience. The ACSC should request contextual details about the specific vulnerability exploited in the cyber incident and actionable information about the nature of the incident, including tactics, techniques, and procedures (TTPs), and indicators of compromise (IOCs).

Incident reporting regulation should enable actionable incident information to be shared with owners and operators of critical infrastructure systems so that they can take steps to protect themselves and seek to mitigate any ongoing attacks. Actionable information sharing across the critical infrastructure sectors would enable owners and operators to help defend against and respond to cyber attacks.

The Australian government should ensure that any national regulation and reporting agencies are adequately resourced to ingest the wealth of information that will be shared by critical infrastructure entities; that they will request and share anonymised data on the types of vulnerabilities that were exploited and the attack paths that adversaries followed after infiltrating target networks; and that they will provide actionable information through trusted partners to provide cyber situational awareness to the broader critical infrastructure ecosystem and enable entities to protect themselves against ongoing and potential attacks.

A single, harmonised portal for reporting cyber security incidents would benefit both regulators and industry, who now face an ever-increasing number of reporting requirements, often with very prompt deadlines, vague and conflicting requirements for the initial report, and a wide range of reporting mechanisms.

Further, many critical infrastructure entities have operations around the world and would be subject to various international cyber incident reporting requirements without a single, harmonised system. Tenable recommends the Australian government engage with foreign governments and regulators to promote the alignment of incident reporting requirements for companies with operations overseas.

16. What opportunities are available for the government to enhance Australia's cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia?

The Australian government can leverage industry expertise and solutions to enhance the country's cyber security technology ecosystem and support the uptake of cyber security services and technologies in Australia. Some potential opportunities include:

1. *Improved visibility and control over cyber risk:* Deploying technology solutions that provide comprehensive visibility into an organisation's IT assets and cyber security posture can help the government identify and prioritise areas where cyber risk is highest. This information can be used to inform policy and investment decisions and support efforts to improve the overall cyber security resilience of the country.

2. *Enhanced threat detection and response capabilities:* By leveraging real-time threat intelligence and automated response capabilities, the government can reduce the time to detect and respond to cyber attacks, minimising the impact on critical systems and infrastructure.

3. *Increased collaboration and information sharing:* The Australian government can leverage the private sector's extensive network of cyber security professionals and industry experts. This network can facilitate collaboration and information sharing between government agencies, industry partners, and other stakeholders, enabling more effective cyber security risk management and response.

17. How should we approach future-proofing for cyber security technologies out to 2030?

To future-proof Australia's cyber security technologies out to 2030, the Australian government should take a proactive approach to cyber security risk management that focuses on:

Assessing and prioritising cyber risks: The Australian government should deploy technologies and solutions to continuously monitor and assess its cyber risks, identifying areas where the risk is highest and prioritising investments accordingly. This will help ensure that the government's cyber security posture remains aligned with emerging threats and technologies.

Emphasising resilience and recovery: In addition to preventing cyber attacks, the Australian government should focus on building resilience and recovery capabilities that enable it to respond quickly and effectively to incidents. The government needs to detect and respond to incidents in real-time, minimising the impact of cyber-attacks and enabling faster recovery.

Embracing emerging technologies: The Australian government should stay abreast of emerging technologies and trends in the cyber security industry, such as cloud security, IoT security, and AI-powered threat intelligence. The government can adopt new technologies and practices that enhance its cyber security posture and ensure it remains at the forefront of the industry.

Collaborating with industry partners: Finally, the Australian government should work closely with industry partners to exchange knowledge and best practices, share threat intelligence, and jointly develop innovative cyber security solutions. By fostering a collaborative approach to cyber security

risk management, the government can leverage the expertise of its partners to address emerging threats and technologies and future-proof its cyber security technologies out to 2030.

Overall, by taking a proactive, risk-based approach to cyber security risk management and collaborating closely with industry partners, the Australian government can future-proof its cyber security technologies and ensure it remains resilient and secure in the face of emerging threats and technologies.

18. Are there opportunities for government to better use procurement as a lever to support and encourage the Australian cyber security ecosystem and ensure that there is a viable path to market for Australian cyber security firms?

Government procurement processes represent a significant opportunity to strengthen the cyber ecosystem and market in Australia. Tenable recommends the government develop enhanced OT-specific cyber security procurement language for use across departments. Currently, public and private sector OT requests for proposals and procurement processes seldom require inclusion of risk-informed cyber security capabilities for products and services. Updating procurement language guidance will help asset owners specify that cyber security must be built into products and projects rather than bolted on as an afterthought. By including cyber security in government procurement vehicles, the Australian government can set a standard that significantly enhances the resilience of critical infrastructure systems nationwide.

The Australian government could also build local cyber security talent by supporting education and training programs in the country. This could include providing scholarships to local students to study cyber security, sponsoring cyber security events and competitions, and providing training and certification programs for local cyber security professionals. One idea is providing additional training funds to enhance the required skills of graduates wanting to work in cyber security.

19. How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?

The Strategy should evolve to address the cyber security of emerging technologies and promote security by design in new technologies by taking a proactive and data-driven approach to ensure that emerging technologies are secure, compliant, and resilient from the outset, protecting both the government and the Australian public from cyber threats. This approach should identify solutions that can help the government to identify and prioritise vulnerabilities and other cyber security risks in emerging technologies, such as Internet of Things (IoT) and connected Operational Technology (OT) devices and cloud-based services. In addition, attaining real-time visibility into emerging technologies would allow the government to identify potential security gaps and proactively address them before they can be exploited.

20. How should government measure its impact in uplifting national cyber resilience?

To measure the impact of uplifting national cyber resilience, the Australian government should establish a set of metrics and indicators that can be used to track progress towards its goals. These metrics should be aligned with the government's strategic objectives for cyber security and should cover a range of areas, including:

1. *Cyber security risk management:* The government should measure the effectiveness of its cyber security risk management programs, including its ability to detect and respond to cyber threats in a timely and effective manner.
2. *Cyber security awareness and education:* The government should track the level of awareness and education among the Australian public and businesses about cyber security threats and best practices.
3. *Cyber security technology adoption:* The government should measure the uptake of cyber security technologies and services among Australian businesses and government agencies, and monitor the effectiveness of these technologies in reducing cyber risk.
4. *Cyber security incident response:* The government should track the number and severity of cyber security incidents in Australia, including the speed and effectiveness of response measures.
5. *Collaboration and information sharing:* The government should measure the effectiveness of its collaboration and information-sharing programs with industry partners, other governments, and international organisations, including the impact of these programs on national cyber security resilience.

By establishing a set of metrics and indicators to measure the impact of uplifting national cyber resilience, the Australian government can ensure that its cyber security investments and programs are effective in enhancing national cyber security resilience and reducing cyber risk for Australian businesses and citizens.

Tenable appreciates this opportunity to respond to these questions and provide some insight and guidance based on our decades of experience in the cyber security industry. Should you have any clarifying questions about the recommendations presented here, we would be happy to provide additional information. Please reach out to Cory Bullock at [redacted]

Sincerely,

Scott Mckinnel
Country Manager, Australia & New Zealand
Tenable, Inc.

James Hayes
Senior Vice President, Global Government Affairs
Tenable, Inc.