14 April 2023

Att: Expert Advisory Board - 2023-2030 Australian Cyber Security Strategy
c/ Department of Home Affairs
PO Box 25
BELCONNEN ACT 2616
Email: auscyberstrategy@homeaffairs.gov.au

2023-2030 Australian Cyber Security Strategy

Fortinet thanks the Australian Government for the opportunity to contribute to the development of the 2023-2030 Australian Cyber Security Strategy[1], which aims to protect and enhance the security and prosperity of Australia in the face of an increasingly complex and evolving cyber threat landscape.

As a global leader in cybersecurity, Fortinet is well positioned to support the Australian Government's efforts to enhance the nation's resilience against cyber threats and safeguard its critical infrastructure, businesses, and citizens. We look forward to working closely with the Australian Government and other stakeholders to make a meaningful contribution to Australia's cyber security posture now and into the future.

Background on Fortinet

Founded in 2000, Fortinet is a US-based developer of novel and next generation security and networking solutions and architectures. Holding more than 1,250 patents, Fortinet is the most innovative provider of cybersecurity and is focused on protecting the breadth of the digital attack surface from edge to core to cloud. In addition to one of the largest threat intelligence organisations in the world, Fortinet leverages analytic expertise, artificial intelligence (AI), and machine learning (ML) systems to analyse security events to protect against ransomware, malware, and other threats. Fortinet secures over half a million enterprises, service providers, and government organisations around the world.[2]

Fortinet is a trusted partner across many industries in Australia, ensuring the safety, security, and reliability of a wide variety of the country's most critical infrastructure. We have an active Common Criteria program of work and develop solutions certified for use by Five Eyes countries. Fortinet strives to support all tiers of government in Australia to ensure that our solutions are fit for purpose. For example, Fortinet has established an Innovation and Integration Centre (IIC) in Canberra to provide sovereign cybersecurity services, customer proof of concept (POC), technical analysis, and SME collaborative opportunities.

[1] 2023-2030 Australian Cyber Security Strategy Discussion Paper (homeaffairs.gov.au)
[2] Learn more about Fortinet and the Security Fabric

Partnering and collaborating with both the public sector and industry has been a cornerstone of Fortinet's strategy for many years. We are a founding member of the Cyber Threat Alliance (CTA), the World Economic Forum's Centre for Cybersecurity, and the MITRE Centre for Threat Informed Defence, three of the leading global forums for cybersecurity collaboration.[3] Fortinet is also a member of the National Cybersecurity Excellence Partnership (NCEP), a US National Institute of Standards and Technology (NIST) program aimed at advancing the state of cybersecurity practice and fostering rapid adoption and broad deployment of integrated cybersecurity tools and techniques to enhance consumer confidence in information technology. We strive to ensure a secure and productive economy for all by working with industry, CERTs, government and academia to proactively share threat information in good faith and protection to raise cyber resilience.

Fortinet would like to offer the following recommendations for consideration, per the discussion questions, posed in Attachment A of the 2023-2030 Australian Cyber Security Discussion Paper:

Detailed Responses: Questions addressed are 1, 2a, 2b, 2e, 2f-g, 4, 5, 7, 8, 9, 12, 13a, and 14.

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?

Fortinet has identified three key areas for consideration:

1. **A focus on global threat intelligence and sharing:** Fortinet's research emphasises the importance of threat intelligence and sharing information about cyber threats among different stakeholders, including governments, industry, and academia. A future strategy needs to prioritise the development of a comprehensive threat intelligence framework and promote collaboration among different stakeholders to improve the country's overall cyber resilience.

   To be effective, cybersecurity must transcend national boundaries. Threat sharing must be more than the current practice of automated sharing of indicators of compromise. Current interactions between government and industry are too often transactional and undermined by lack of trusted processes and procedures. A framework must be created that facilitates, supports and nurtures transparent, win-win relationships between government and industry.

   Today's sharing must evolve to genuine, trusted, collaborative partnerships, whereby Australian entities are able to benefit from the expertise of local and international

[3] Centre for Cybersecurity > Platforms | World Economic Forum (weforum.org)

899 Kifer Road
Sunnyvale, CA 94086
Tel: +1-408-235-7700
Fax: +1-408-235-7737
www.fortinet.com

specialists residing in these companies. Good, timely and actionable data, with expert assessment with regard to local context will bring genuine benefit.

2. **A focus on emerging technologies:** The full benefit of emerging technologies such as AI, quantum, etc. will only be realized if security is addressed at every stage from research through design, production and use of solutions. Any future strategy needs to prioritise development of policies and guidelines that promote secure adoption of these technologies, including measures such as secure-by-design principles, vulnerability management, and security assessments. It is essential to work with trusted vendors who prioritise security and are committed to ongoing security improvements.
3. **Better cybersecurity education and awareness:** Fortinet supports the need for better cyber security education and awareness among the general public, including individuals, businesses, and government agencies. The strategy must prioritise developing and/or better utilising existing programs and initiatives that promote cybersecurity literacy and awareness, including targeted education campaigns and public-private partnerships.

2(a): What is the appropriate mechanism for reforms to improve mandatory operational cyber security standards across the economy (e.g. legislation, regulation, or further regulatory guidance)?

Fortinet supports further development of proactive best practice standards in cyber security and a consistent approach to cyber specific legislative or regulatory obligations across industry and government. Australia's approach should recognize that cyber security is dynamic and may countering threats often requires actions that do not align with local and international borders.

The more aligned and consistent Australia's legislation can be with key international partners' legislative or regulatory frameworks, the more Australia's effort will encourage and support the creation of more trusted and secure international cyber secure supply chains.

There is significant opportunity for Australia to leverage the world leading security solutions and expertise residing in companies like Fortinet, and to partner on initiatives to educate and support end users to ensure that the people, processes and technology are as secure and resilient as possible. Government and key technology creators in industry should leverage their resources to help Australian business deliver better cyber by default. This should include a clear articulation by the government of cyber 'due diligence' standards that should be accompanied by an offer from government of safe harbor if an entity follows these models and best practices in good faith and has a problem nonetheless.

2(b): Is further reform to the Security of Critical Infrastructure Act required? Should this extend beyond the existing definitions of 'critical assets' so that customer data and 'systems' are included in this definition?

This SOCI Act is a very good starting point to stimulate increased resilience in Australia's most critical systems and supply chains. The key next step is to better understand the links, interdependencies and cyber gaps in these systems at a macro level.

Australia's national security is likely to be stress tested over the coming years due to the changing regional geostrategic order. In fact, it is certain that some of these Critical Systems are already being compromised by sophisticated actors in "grey zone" activity – primarily espionage and prepositioning for (current) commercial advantage; and (future) state manoeuvres. For example the recent US Annual Threat Assessment [4] provides clear commentary on the cyber capabilities of Russia, China, North Korea and Iran and broader assessments such as "*Foreign intelligence services are adopting cutting-edge technologies—from advanced cyber tools to unmanned systems to enhanced technical surveillance equipment—that improve their capabilities and challenge U.S. defences. Much of this technology is available commercially, providing a shortcut for previously unsophisticated services to become legitimate threats*".

The current legislation needs to move beyond these three constraints:

1. The Security Requirements are quite modest, and will be insufficient to protect critical infrastructure from a motivated, sophisticated threat actor;
2. The current legislation puts all financial, implementation and operational burden on the critical infrastructure operators. This will lead to solutions that are constrained by price, and by a lack of expertise and cyber resources in the market. A model that is better supported by both government and industry resources and expertise is realistically much more likely to drive real resilience into some of these fragile systems; and
3. There is no government entity with a macro level view or understanding of the interdependences and risks to Australia's whole-of-nation cyber security. The current legislation assumes that industries will improve cyber hygiene through legislative requirements and provides support if and when an incident occurs – but the requirements are modest, and the support is reactive. A combined government and industry body that is able to model and exercise macro-level systems and test effects-based disruptive events will identify gaps that, if addressed, will improve national cyber resilience. Additionally, the experts residing in that community would become a vital asset to the Australian Cyber Security Centre, the Critical Infrastructure Centre and the other broad range of critical infrastructure stakeholders and risk owners.

[4] ATA-2023-Unclassified-Report.pdf (odni.gov)

2(e): How should Government seek to monitor the regulatory burden on businesses as a result of legal obligations to cyber security and are there opportunities to streamline existing regulatory frameworks?

Fortinet supports the Australian Government in creating a National Office for Cyber Security and a Coordinator for Cybersecurity. These new functions will help to address the need for a consistent national approach to cyber security. It will be important to initially identify (through industry engagement) any duplication or overly complex legislation that is creating uncertainly/issues for Australian businesses, in particular small and medium enterprises. The cyber security strategy should address, for example, that a core objective of the National Office for Cyber Security is to evaluate current and future regulations to ensure it will not result in overly complex compliance requirements or duplication across jurisdictions.

The cyber security private sector has a long history of collaboration, in particular on cyber-crime threat intelligence sharing, and this cooperative approach should be leveraged when looking at cyber security regulatory frameworks. The establishment of an industry consultation body, with a rotation of membership of relevant industry bodies and individual companies, could provide real life insights and understanding of how the regulatory framework is operating for Australian policy makers.

2(f)-(g): 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? What impact would a strict prohibition of payment of ransoms and extortion demands by cyber criminals have on victims of cybercrime, companies and insurers? 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?

Fortinet recommends a consist global approach to the payment of ransomware where payment is discouraged but not prohibited (similar to how some countries approach payments in the case of a kidnapping). If a victim has cyber insurance coverage for the ransom payment, the use of this insurance should be allowed. These payments need to be reported to the Australian Government to enable more accurate intelligence/threat assessments.

While paying the ransom must remain a business decision for the victim based on individual context, there is a gap in how victims are supported before, during and after a ransomware incident. A proactive reporting and support capability that the victim could engage for advice when in crisis would be extremely beneficial. This capability could assist in negotiations with the threat actor, as well as collect valuable intelligence to support a subsequent law enforcement prosecution.

899 Kifer Road
Sunnyvale, CA 94086

Tel: +1-408-235-7700
Fax: +1-408-235-7737

www.fortinet.com

4: What opportunities exist for Australia to elevate its existing international and multilateral partnerships from a cyber-security perspective?

As a global company Fortinet supports the Australian Government's focus to elevate itself as a leader in cyber security while uplifting and deepening its international relationships. This is particularly important based on the current geo political environment. Many multilateral and bilateral agreements already address cyber security matters including the recent cyber security discussions with the QUAD[5].

It will be important as the Australian cyber security strategy is finalised that there is alignment with other likeminded countries' cyber security legislation to avoid compliance and reporting confusion, inconsistences and unnecessary complexities for companies operating in multiple countries.

There is an opportunity for the Australian Government to increase and have stronger private-public engagement a part of these international partnerships and leverage the global cyber security forums and alliances already established.

Fortinet for example is a member of various industry alliances and organisations, including Cyber Threat Alliance (CTA)[6], MITRE Centre for Threat-Informed Defence[7], World Economic Forum – Centre for Cybersecurity[8] and the NIST's National Cybersecurity Excellence Partnership (NCEP)[9] that work towards promoting industry standards, sharing threat intelligence, advancing cyber security research and development and the potential to advance the state of cyber security practice.

5: How should Australia better contribute to international standards-setting processes in relation to cyber security and shape laws, norms, and standards that uphold responsible state behavior in cyberspace?

Rapidly emerging or evolving technologies continue to have the potential to disrupt traditional business and society with both positive and negative outcomes, while creating unprecedented vulnerabilities and attack surfaces.[10] It is critical that Australia contribute to shaping this process given the emergence of competing visions of the role of the Internet and Information and communication technology . The private sector has the expertise and numbers (of potential participants) that government may lack. While any private sector

[5] Quad Senior Cyber Group (homeaffairs.gov.au)
[6] Home - Cyber Threat Alliance
[7] Center for Threat-Informed Defense Releases Impact Report, Illustrating Collaborative R&D Approach in Cybersecurity | MITRE
[8] Centre for Cybersecurity > Platforms | World Economic Forum (weforum.org)
[9] Collaborate with Us: Technical Contributions | NCCoE (nist.gov)
[10] ATA-2023-Unclassified-Report.pdf (odni.gov)

participant usually speaks only for itself, the Strategy can try to create systemic opportunities to enable them to be representatives of a sector or even national positions, based on pre-coordination (e.g. use of sector-focused councils and/or collaboration with Government).

Australia should continue to emphasise the important role of international cyber security standards in facilitating interoperability of approaches and securing cyberspace globally. Cyber security standards (like the ISO 27000 series) developed by Joint Technical Committee 1 (JTC1) of the International Standards Organization (ISO) and the International Electro technical Commission (IEC)[11] have guided the global IT industry for 35 years.

In work with international partners, Fortinet is involved in global discussions aimed to disrupt the support structures exploited by cybercriminals. Much of this discussion is currently undertaken in parallel to government to government discussions. Better identification, mapping and connection of comparable activities would lead to more impactful results and a reduction in duplication of effort.

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

Building cyber resilience should be shared responsibility between government and all sectors of industry – in particular with critical infrastructure operators, service providers, and cybersecurity companies. Strong public-private partnerships are essential in protecting Australia's critical infrastructure and will offer more focused, practical, and cost-effective new technology.

The continue development of the Australian Cyber Security Centre (ACSC) collaboration opportunities for greater involvement of industry in threat sharing is important.

For example, Fortinet's threat intelligence and research organisation provides threat intelligence services that help organisations identify risk and strengthen security. Our threat research and response team is made up of expert analysts globally who identify new or unknown threats and develop ways to detect them before they become entrenched in customer networks. We have also discovered more than a thousand 'zero day exploits'[12], which are attack techniques that were previously unknown. This intelligence and research is gladly shared currently with the Australian Government and we would welcome increased partnership opportunities. The Australian Government overall should ensure the full utilisation of the data and research produced by the private sector.

Current systems such as the ACSC CTIS system are maturing and becoming much more effective. They could be strengthened by expanding on opportunities to build a community

[11] Understanding standards | IEC
[12] report-2023-threat-landscape.pdf (fortinet.com)

of experts. CTIS is able to share Indicators of Compromise, but a community that is able to share context, expertise and collaborate would be an order of magnitude more powerful. Additionally, global organisations like Fortinet have a local footprint, but also can connect Australian defenders with expert colleagues across the globe to facilitate learning and assistance.

8: During a cyber-incident, would an explicit obligation of confidentiality upon the Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC) improve engagement with organisations that experience a cyber-incident to be shared between the organization and ASD/ACSC without the concern that this will be shared with regulators?

Fortinet believes that an explicit promise that information disclosed will not be used for regulatory purposes is vital. Also important is a guarantee that information shared externally to government will be anonymized and identity protected (e.g. this is particularly important for reputational damage and commercial competitiveness).

The private sector will likely be more favourable to engagement and openness with government when confidentiality is guaranteed. The government should also ensure that the information will not be utilized for regulatory purposes. These two points should help maximise collaboration and capture the broadest partner base and data points.

9: 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?

Fortinet supports mandating reporting of ransomware. To be effective, the threshold limit must not be too low, the required data should not be too onerous for the business to provide and the timeframe for reporting cannot be too fast. This data can be an invaluable resource for gauging the magnitude and impact of threat activity and the effectiveness of response measures.

Rules of engagement must also be established to ensure that victims of cybercrime are not politicised or victim shamed. The reality is that cyber defines is extremely challenging, threat actors are sophisticated and prolific, and mistakes will be made.

After such an incident or reporting, the key aim must be damage minimisation, followed by education and improvement. The Unites States Solarium Commission in 2020 proposed

a Bureau of Cyber Statistics (BCS)[13] to be established in the United States which would serve as a repository of national data on cybersecurity incidents. This in turn would help both public and private sector organisations inform their risk-based decision-making and cyber strategy planning. This has not yet been implemented in the US but this type of centralised portal should be considered as part of the new National Office of Cyber Security remit.

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

The "human element" is an important part of cybersecurity. By itself, technology cannot provide the answer to cyber threats. As such, training is a vital part of cyber defines to ensure stronger data protection by increasing understanding of the latest threats and possible solutions.

It is also increasingly essential that cyber training moves out of the IT department and becomes a foundational requirement for all employees. Cyber training must be made relevant and engaging for our current and future workforce[14]. Australians will only become more IT connected, so basic cyber awareness should become more of a foundational skill instilled across all age groups.

Cyber security training should also be extended to all parts of our economy. That means business partners and subcontractors—essential partners in delivering a working economy, critical infrastructure, and national security infrastructure—must be trained and committed to protect data from cyber threats. Working with a highly qualified partner with comprehensive cybersecurity training will help prepare Australia to deal with risks and threats in its systems, networks, and devices.

Many cyber security companies can support the Australian Government with cyber security training. For example, the Fortinet Training Institute is committed to developing experts in the field of cybersecurity through training and certification. The Training Institute's certification program enables people to learn about cybersecurity at all levels, ranging from awareness to foundational to expert level knowledge. Supported by Fortinet's strong network, the Training Institute has issued more than one million certifications to date. Fortinet's Academic Partner Program and Education Outreach Program work with higher education as well as non-profit and government initiatives. Through these programs, Fortinet offers training and certification opportunities for women, veterans and military spouses, students, and economically disadvantaged individuals in order to cultivate a more diverse, equitable, and inclusive cybersecurity workplace. Fortinet offers all its self-paced training

[13] Cyberspace Solarium Commission - Report
[14] 3R8N1DZJ (ibm.com)

courses for free, which includes over 300 hours of curriculum. To continue its work to help close the cybersecurity skills gap, Fortinet has pledge to train one million people over the five-year period from 2022-2026.

The Australian Information Security Association recently conducted a survey on accreditation with its members – and the concept was strongly rejected.[15] The cyber security industry is extremely diverse, with some of the current leaders from diverse backgrounds such as law, international relations, social science. This is especially critical with a sector that experiences resource shortages and lacks appropriate diversity, especially with female practitioners. The lack of representation of women in STEM is a difficult challenge, but the cyber industry can work around this through a more open and diverse passage to entry and broader career paths.

13(a): Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?

Fortinet supports the establishment of a single portal for reporting cyber security incidents which would benefit both government and industry. Having all reporting obligations into a signal portal would increase efficiency for businesses during an often a highly stressful time, increase the accuracy of information provided, and reduce the risk of conflicting and duplicative reports for regulators.

By having a single portal, the opportunity for a Bureau of Cyber Statistics type organization (refer to Q9 answer) to provide meaningful analyses for future policy considerations can occur and in turn will demonstrate to both the private sector and general public the value of contributing to a central portal.

A single point of entry would be valuable, but the information within must be managed with extreme care. Anonymization and protection of victim data will be essential both for encouraging victims to report and to avoid the portal becoming a potential targeting list for malicious actors.

14: What would an effective post-incident review and consequence management model with industry involve?

In 2022 the United States created a Cyber Safety Review Board[16] which is composed of both government and private sector representatives. Its primary role is to investigate major cyber security incidents/events and make recommendations to improve cyber security for both the

[15] AISA Accreditation Survey Report 2022
[16] Cyber Safety Review Board (CSRB) | CISA

public and private sector. The Board has a direct reporting path to the Secretary of Homeland Security and the United States President and has provided already valuable post action reports outlining actionable recommendations for how organisations can protect themselves, their customers and their employees. This type of board as part of the Australian cyber security strategy would promote stronger public/private engagement post a major cyber incident.

In Conclusion

Fortinet thanks the Australian Government, through the Expert Advisory Board, for providing the opportunity to provide feedback on the 2023-2030 Australian Cyber Security Strategy - Discussion Paper. We appreciate the government's recognition of the importance of cyber security and focus to address this critical issue. We are committed to supporting the Australian Government in this mission and look forward to continuing our collaboration to enhance the Australian cybersecurity landscape.

Fortinet would be very happy to discuss our ideas further with the Expert Advisory Board moving forward. For further follow-up or information please contact Nicole Quinn, Head of Government Affairs – APAC at

899 Kifer Road
Sunnyvale, CA 94086

Tel: +1-408-235-7700
Fax: +1-408-235-7737

www.fortinet.com