NCC Group's response to the 2023-2030 Australian Cyber Security Strategy Discussion Paper

April 2023

Introduction

NCC Group welcomes the opportunity to respond to the 2023-2030 Australian Cyber Security Strategy Discussion Paper and to offer our expertise as a global cyber security business.

Through our threat intelligence, incident response and research functions, we are acutely aware of the cyber threat landscape, witnessing first-hand the real-world impact cyberattacks have on their victims, communities and ecosystems. **While Australia is, in many ways, at the forefront of cyber resilience (e.g. through its leadership of the International Counter Ransomware Initiative), we support the Government's focus and drive to establish cyber security as a strategic national capability**. In this response, we put forward practical considerations and recommendations for protecting businesses, the public sector and citizens at scale, enabling them to thrive in the digital age. It is vital that the Government uses all its levers to prioritise and manage cyber threats, in partnership with the private sector, driven by a culture of information sharing and open dialogue.

Principally, we advocate for a National Cyber Security Strategy that:

- Establishes the evidence-base needed to make informed decisions on cyber security policies, through the formation of a **Bureau for National Cyber Statistics**.
- Through the new Cyber Security Act, embeds a **consistent, proportionate and risk-based 'secure by default' approach** across all parts of the economy.
- For the most high-risk sectors, mandates the **adoption of realistic, intelligence-driven cyber security assurance testing**.
- Implements a **security labelling scheme for consumer IoT devices**.
- Encourages **public and private sector collaboration**, including industry secondment schemes like the Industry100 programme delivered by the UK National Cyber Security Centre. As participants in the Industry100 programme since its inception, we would be delighted to support the Australian Cyber Security Centre (ACSC) to establish an equivalent scheme here in Australia.
- Promotes close **cooperation and collaboration with global allies**, particularly the 'Five Eyes'.
- **Improves cyber literacy** so that all levels of society, age groups and professions can use technology securely.

We are pleased that the Government is taking the time to review its approach through to 2030, and we are keen to support the development of a new Strategy by sharing our expertise and insights from operating at the 'coalface' of cyber security. Below we explore our recommendations in more detail, responding directly to the Discussion Paper's questions.

About NCC Group

NCC Group's purpose is to create a more secure digital future**.** As experts in cyber security and risk management, our 2,000+ people worldwide are trusted by our customers to help protect their operations from cyber threats. Each year we dedicate thousands of days of internal research and development enabling us to stay at the forefront of cyber security and ensuring we secure the rapidly evolving and complex technological environment. As a global business operating in 12 countries, we were delighted to open our regional headquarters in Sydney last year amid a rapidly growing footprint across Australia, with around 90 colleagues now based here.

Response to questions

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?**

At an international and national level, **we support the Government's intent to disrupt sophisticated threats (projection of hard power) and deter threat groups from attacking Australia (projection of soft power)** through deliberate action and international cooperation. The cyber threat landscape is complex, involves many actors and the complicit involvement of nation states, with cyberattacks very rarely originating from Australia alone. In addition, even if Australia was impervious to cyberattacks, overseas suppliers – many of whom are critical to the functioning of the economy and critical national infrastructure – may not be. **Close international cooperation is therefore critical to ensuring a secure and trusted global supply chain for Australia's economy** and this should be front and centre of the Government's policy discussions when developing its approach. Specifically, we recommend that the Government:

- Utilises existing successful partnerships, including the 'Five Eyes' alliance and the International Counter Ransomware Initiative (CRI), strengthening global cooperation and coordination against malicious actors.
- Invests time in developing practical outcomes with other governments, that go deeper than high-level principles – such as information sharing, free movement of security professionals and the removal of tariffs concerning security services and products.
- Ensures that civil society and industry - who will play a central role in delivering the Governments' objectives - are involved in discussions from the outset.
- Works with partners to disincentivise and disrupt the financial flows of ransomware actors, through greater regulation of crypto exchanges, individual indictments and red notices and enhanced coordination across borders.

In addition, we believe the Government should create **a new Bureau of National Cyber Statistics** - a centrally coordinated institution to bring together existing and new datasets to build a full picture of the cyber threat landscape. This would enable the Government to more effectively communicate the true scale of the threat to the public, prioritise actions, allocate resources and measure the success of Government efforts. As US National Cyber Director Chris Inglis recently commented[1] when speaking about similar considerations in the US, "to properly address risk, we have to first understand it, we have to understand where it's concentrated, where it cascades, what causes it, and more importantly to then discover how to address it."

At an industry level, we welcome the Government's ambitions for Australian-made products to set the international benchmark for safety and security, while balancing consumer rights and economic competitiveness. To that end, we support the introduction of a new **Cyber Security Act**. We hope this Act will introduce a consistent, proportionate and risk-based 'secure by default' approach across all parts of the economy that:

- (As the Minister for Home Affairs has already laid out[2]) Removes, as far as possible, end-user responsibility for their cyber security online, providing a safety net for the least technically-inclined users, more readily enabling them to confidently participate in digital society.
- Creates a framework for identifying the most high-risk products and services (such as those more vulnerable to cyberattacks or those which present safety concerns, like autonomous vehicles) which will be subject to increased regulatory oversight. In practice, this would mean greater supervision to ensure compliance with a higher baseline of mandatory cyber resilience requirements, building on evidence from the ACSC, as well as the **greater use of realistic, intelligence-driven cyber security assurance testing.**

[1] https://fcw.com/security/2021/08/national-cyber-director-backs-new-bureau-of-cyber-statistics/258952/
[2] Australian Information Security Association's (AISA) Australian Cyber Conference 2023 (homeaffairs.gov.au)

- Builds on the voluntary set of measures set out in the Australian Government 'Code of Practice: Securing the Internet of Things for Consumers' to **improve the security of IoT devices** in Australia, moving towards Singapore's Cybersecurity Labelling Scheme (CLS) with registration for manufacturers, approved labs and clear labelling as to the met levels of security within the products for consumers. A phased approach could be implemented for more high-risk products, like consumer home wireless routers and privacy related IoT devices, without overlapping with the Australian Information Security Evaluation Program (AISEP) product evaluations for commercial grade products. The Government should also establish MoUs with other like for like schemes in other parts of the world.
- Brings together federal and state laws under one consistent framework.
- Aligns closely with Australia's global security partners.

A close partnership between Government and industry is essential to delivering a reliable and resilient cyberspace. We are therefore pleased to see this reflected throughout the Discussion Paper. Crucial to this will be an **ever-closer cooperation between the ACSC and the cyber security sector, including through capacity building initiatives**. NCC Group is proud to be a long-standing partner to the UK National Cyber Security Centre (NCSC), supporting its strategic and operational missions to improve cyber capability, develop skills and support growth. This has included participating in and helping to shape its Industry100 scheme which brings industry staff together with NCSC teams on a part-time basis to enhance collaboration between government and industry, and to build public sector cyber capacity. We would be pleased to meet with the Expert Advisory Board / Department of Home Affairs to share our experience, should this be of interest.

At a public level, empowering individuals and users to make informed decisions about their personal security should be a core part of the Government's approach (particularly when you consider that, despite best efforts to mandate security, cheap insecure products will likely continue to be sold to Australian consumers through online marketplaces). We believe a step change is needed further to embed cyber awareness and incentives into everyday conversations, to make it an integral part of the national psyche. At the heart of this should be the concept of 'pervasive cyber literacy' - a basic level of cyber competence across all levels of society, age groups and professions to allow everyone to use technology securely. This could involve:

- A renewed focus on the people element of cyber security, developing human cyber risk awareness and skills; and their interactions with technology or human factors.
- Starting cyber education and awareness in early school years.
- Including cyber competence, covering safe and secure online behaviours, privacy, and use of technology alongside broader technology and computing lessons, as a mandatory part of the school curriculum. This should be reviewed and tested with an industry advisory board on a regular basis to ensure it keeps pace with technological developments and industry requirements.
- Applying the lessons of a safety-first culture to the cyber challenge across all domains by requiring mandatory basic cyber security training as part of individuals' induction upon their entry into the workforce.

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

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)?

As part of a proportionate risk-based approach, the Government should, where appropriate and sufficient, introduce legislation to provide clear guidance to businesses and the community regarding the standards it expects. For example, if there is an implied consideration or obligation on Directors

(see response to 2c), they may be compelled to implement guidelines, steered by information criticality and threat sophistication.

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

In principle, we support the extension of SOCI; however, further assessment of the suitability, acceptability and feasibility of an extended scope is needed, in consultation with industry.

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

To ensure tangible results, any obligations would need to be placed on the Board, and on Directors and Officers in exercising their duties to the company. This could be done via the new Cyber Security Act or via an amendment to the Corporations Act, through including a positive obligation to consider cyber security as part of the suite of Directors' duties. Under the Corporations Act, directors are required to exercise their powers and perform their functions:

- in good faith including acting in the best interests of the company;
- with care and diligence; and
- without using their position or information to gain personal advantage (ss 180, 183, 601FD).

It could be argued that, in the current climate, consideration of cyber security is implied, and the regulators could bring an action arguing an implied duty; however, this would have to be tested in court through costly litigation at the expense of a regulator or shareholder class action. Parliament, however, has the unique power to insist upon directors an explicit obligation to elevate the duty to consider cyber risk.

d. Should Australia consider a Cyber Security Act, and what should this include?

Yes. As outlined under question 1, such an Act should introduce a consistent, proportionate and risk-based 'secure by default' approach across all parts of the economy. It should seek to align with similar regimes in allied regions and, as far as possible, remove end-user responsibility for their cyber security.

In high-risk sectors, where the impact of a cyberattack would be greater (for example, for critical national infrastructure), we believe there is a need for more widespread adoption of realistic, intelligence-driven cyber security assurance testing. The value of such testing has been clearly demonstrated in the financial services space by the Cyber Operational Resilience Intelligence-led Exercises (CORIE) framework led by the Council of Financial Regulators. The scheme allows the participants, regulators, ACSC and the Government to understand the cyber risks and resilience issues and respond to the needs of the sector. They are intelligence-led, so the ethical attack teams replicate the tactics, techniques and procedures of known threat actors. Organisations learn what and how attacks could have an impact, assess their ability to detect and respond and measure the return of their investment and training in improving their cyber resilience. Meanwhile, regulators gain important insight as to the actual real-world resilience and risk to their sector.

e. How should Government seek to monitor the regulatory burden on businesses as a result of legal obligations to cybersecurity, and are there opportunities to streamline existing regulatory frameworks?

A centralised Cyber Security Act would go some way toward providing consistency and clarity for businesses, thereby reducing the regulatory burden.

Additionally, a phased approach could be adopted, ensuring that the industries or businesses facing the largest exposure or risk adopt measures sooner. For example, the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 adopted such a phased approach whereby authorised deposit taking institutions, gambling organisations and gold bullion dealers were the first to be regulated as part of tranche one, as these organisations have the greatest exposure to financial crime risk. Tranche two will extend to the next most at-risk group (gate keepers such as lawyers, real estate agents, accountants etc). A similar approach could be adopted for the proposed cyber security legislation, however, given the speed at which technology moves we would suggest taking a more expedient approach between phases.

We also advocate greater alignment of sector-specific regimes to strengthen critical infrastructure's overall operational resilience. While we note that this Discussion Paper looks primarily at managing cyber resilience, the digitalisation of the economy and increasing reliance on third-party software and cloud providers creates a complex risk landscape that extends beyond cyber risk to supplier failure, concentration risk and service deterioration. Some regulators, such as the Australian Prudential Regulation Authority[3] (APRA), are updating their guidelines to ensure critical infrastructure providers like banks and the insurance industry are managing these interrelated risks effectively. With operators increasingly reliant on their software supply chain, we believe other regulators overseeing critical sectors should follow suit. Within the financial services sector, NCC Group has been at the forefront of regulatory discussions around mitigating the ramifications of supplier failure through the adoption of the 'Resilience by Design' concept. This assumes supplier failure by default, regardless of their risk profile, and encourages or mandates escrow agreements[4] as a proportionate and cost-effective mitigation against supplier failure. We would welcome the opportunity to discuss how 'Resilience by Design' could be adopted across the economy in more detail.

f. Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals by: victims of cybercrime; and/or 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?

We believe that these measures warrant further exploration; however, any ban would need to be carefully considered, in close consultation with industry. We are particularly concerned that bans and exceptions for at risk services (e.g. human life related or public services) may lead to potential inadvertent consequences such as their specific targeting. We have observed how related threat groups have rapidly evolved to changes that affected their success or freedoms. Any legislation to impose bans should anticipate such responses. The problem is compounded with the complexity introduced when nation states use ransomware to mask other objectives.

Beyond ransomware payment bans, the Government should consider how it could use all statecraft tools at its disposals, working with partners (e.g. through the International Counter Ransomware Initiative), to disincentivise ransomware actors at scale. This should include cross agency support from the Justice Department, Law Enforcement and the Treasury to impose arrest warrants, extraditions and sanctions. Penalties and sanctions should be extended to organisations helping groups launder illicit funds.

g. 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. Clarity and conviction is needed.

[3] APRA consults on new prudential standard to strengthen operational resilience | APRA

[4] Cloud, software and technology escrow agreements are resiliency solutions offering a minimum level of resilience through legal and technical means to ensure continuity of services while a service is being restored and/or alternative options are being implemented.

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

We couldn't agree more that looking beyond Australia's physical borders is needed to build a resilient cyberspace. To that end, we recommend:

- Greater information sharing, including improving quality and availability of sectoral and threat data to enrich predictive and automated response.
- Further investment in x-Border security, business continuity, disaster relief and law enforcement networks, including: regional exercises to stress test strategic lines of communication (building on the work already ongoing with critical national infrastructure); and, co-developing good practice for response to securing emerging technologies and new markets.
- Educating Australian organisations that import and export technology products – focusing on the value created by secure and privacy by design frameworks, and supply chain risk management. This could include requiring importers and exporters to promulgate the message to their consumers or suppliers.

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

As outlined under question 1, collaboration and alignment with global security partners should be an essential tenet of the Government's approach. Specifically, we recommend that the Government:

- Utilises existing successful partnerships, including the 'Five Eyes' alliance and the International Counter Ransomware Initiative (CRI), strengthening global cooperation and coordination against malicious actors.
- Invests time in developing practical outcomes with other governments, that go deeper than high-level principles – such as information sharing, free movement of security professionals and the removal of tariffs concerning security services and product.
- Ensures that civil society and industry - who will play a central role in delivering governments' objectives - are involved in discussions from the outset.
- Works with partners to disincentivise and disrupt the financial flows of ransomware actors, through greater regulation of crypto exchanges, individual indictments and red notices and enhanced coordination across borders.
- Builds attractive ecosystems (in city hot spots), promoting and funding opportunities for tech and cyber start-ups and gaining from foreign direct investment and inward migration.

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 behaviour in cyber space?

We recommend that the Government:

- Encourages Australian industry experts to take a leading role in international industry bodies such as CREST[5], ISACA[6], and within established institutions like the World Bank, IMF, OECD and the United Nations. Industry can play a key role in shouldering the responsibility of building a secure global cyberspace and amplifying Australia's soft power abroad, particularly where there is clarity of mission.
- Participates in defence and national exchange programmes.
- Hosts and runs security incubators and accelerators.

[5] Home Page - CREST (crest-approved.org)
[6] In Pursuit of Digital Trust | ISACA

6. **How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice, and what can government do to improve information sharing with industry on cyber threats?**

As outlined above, a close partnership between Government and industry is essential to delivering a reliable and resilient cyberspace. This should include industry secondment schemes like the Industry100 programme delivered by the UK National Cyber Security Centre. As participants in the Industry100 programme since its inception, NCC Group would be delighted to support the Australian Cyber Security Centre (ACSC) to establish an equivalent scheme here in Australia.

7. **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 so as to allow information to be shared between the organisation and ASD/ACSC without the concern that this will be shared with regulators?**

If sharing of the information is deemed critical to national recovery and an established obligation provides control protections during 'data processing/transmission' in the present – then, yes. If a regulator (involved typically at post-incident investigation) requires information, it can request/demand it from the data owner as part of arbitration or legal proceedings.

8. **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?**

Potentially. Although further consideration would be needed as to what is meant by an "incident" to ensure that organisations and regulators are not burdened with thousands of incident reports a day.

Equally, it is our view that it is not so much the public who require a comprehensive understanding of the threat landscape, but rather those organisations that are able to act on it. As we have outlined elsewhere, while the public should be empowered and upskilled to make decisions about their own digital security, we believe that responsibility for security should (as far as possible) be removed from end-users, providing a safety net for the least technically-inclined users.

That said, we believe there is scope for a centrally coordinated effort to bring together existing and new datasets to build a full picture of the cyber threat landscape. We therefore propose establishing a Bureau of National Cyber Statistics that anonymises, collates and disseminates incident data from all sources.

9. **What best practice models are available for automated threat-blocking at scale?**

Zero-trust architecture and network zoning (e.g. the Azure Well-Architected Framework), as well SOAR (Security Orchestration, Automation, and Response), are best practice. The Government should also consider the role of evolving machine learning and artificial intelligence solutions. There may also be scope to work more closely with global allies to share best practice and solutions.

10. **Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda? 12. What more can Government do to support Australia's cyber security workforce through education, immigration, and accreditation?**

Yes. As outlined under question 1, we believe more can, and should, be done to drive up cyber literacy across Australia – not only so that we train the cyber professionals of the future but also to ensure everyone has the cyber skills they need to thrive in the digital age.

In addition, industry has a key role to play in increasing overall literacy and workforce capabilities, so long as it is supported to identify those with the right aptitude and attitude, and there is investment in ensuring graduates and school-leavers have the skills they need to enter the workforce.

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

As outlined above, we support a Cyber Security Act that embeds a proportionate and risk-based 'secure by default' approach across all parts of the economy. As potentially high-risk products, cyber security technologies should also undergo resilience testing that emulates threat actors prior to production.

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?

Yes. The Government should review transparency and competitiveness on government panel arrangements and ease of access to public sector contracts for new firms. With the recent consolidation of the cyber security services market and the average age of Australian cyber security firms being relatively young, the Government must consider whether the ecosystem is still performing fairly and effectively, as intended.

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

As outlined above, we support a Cyber Security Act that embeds a proportionate and risk-based 'secure by default' approach across all parts of the economy. This extends to emerging technologies. Indeed, the law should be designed to keep pace with modern technological and societal developments by building-in flexibility, agility and periodic regulatory and legislative reviews from the outset and investing in coordinating and improving horizon-scanning. This ideally should include requirements for regulators and policymakers to engage regularly with innovation centres and industry experts.

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

As outlined under question 8, we believe the Government should create a new Bureau of National Cyber Statistics - a centrally-coordinated institution to bring together existing and new datasets to build a full picture of the cyber threat landscape. This would enable Government to prioritise actions, allocate resources and measure the success of efforts.

Other measures could include the (safe) adoption of new technologies, the uptake of security standards, economic growth of the cyber security industry, saturation of academic courses in schools and universities and graduate and employment numbers.

21. What evaluation measures would support ongoing public transparency and input regarding the implementation of the Strategy?

The Government should establish measurable evaluation criteria against Strategy pillars and an implementation timeline. To support the measurement of progress, the Government could consider collecting feedback from industry, government, communities and residents to inform an impact analysis. Focus groups could also be used in the interim to understand perceived delivery and adjust direction as necessary.