NCC Group's response to Horizon 2 of the 2023-2030 Australian Cyber Security Strategy

August 2025

Executive summary

NCC Group welcomes the opportunity to respond to the Department of Home Affairs' consultation and offer our expertise as a global cyber security business.

Horizon 1 of the Cyber Security Strategy has brought about many positive changes, from long overdue updates to the SOCI Act and smart device standards to global leadership through the Counter Ransomware Initiative (CRI) and successful law enforcement takedowns. However, against an unstable geopolitical backdrop, the rate, severity and sophistication of cyberattacks and hybrid threats continues to grow. We also see nation states doubling down on developing strategic, sovereign cyber and emerging technology capabilities.

A collective response is required to ensure that Australia has the right capabilities, institutional structures and legal frameworks to stay ahead of emerging threats and create a flourishing digital economy. We are therefore pleased with Horizon 2's focus on cyber security as a 'team sport'. In practice, this must strike the right balance between mandated rules, empowerment initiatives and proactive support – recognising the different needs and resources of organisations across the cyber ecosystem and wider economy. In particular, we advocate for a Horizon 2 that prioritises the following policies:

- **A proportionate globally-aligned regulatory response** to emerging threats and technologies and the changing economic landscape, including an **AI Act for Australia**, further **updates to SOCI** and extending and requiring the Cyber Trust Mark for all digital products used in Australia's public sector and critical infrastructure.
- A detailed and continually updated **national PQC roadmap**, signalling to both public and private sector organisations what they need to achieve and by when.
- Appropriate **support for small and medium-sized businesses (SMBs) and non-profits**, building on the success of the Small Business Cyber Resilience Service.
- Development of **shared capabilities with Five Eyes, AUKUS and other regional allies**, because cyber security as a 'team sport' applies globally as much as it does domestically.
- A centralised **national cyber skills strategy**, that creates the cyber professionals that we need today and tomorrow, while also ensuring all citizens from board members to school-age children have the cyber literacy skills they need to make informed decisions about their digital security.
- An **ever-closer public-private partnership** between the Government and the cyber security sector, including through co-creation of capabilities, regular feedback mechanisms, two-way secondment schemes and improved information sharing.
- **Legal clarity on permissible unauthorised access** to computer systems, both in terms of Active Cyber Defence but also security vulnerability research.

About NCC Group

NCC Group's purpose is to create a more secure digital future. As experts in cyber security and risk management, our c.2,200 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, our regional Asia Pacific headquarters is based here in Sydney.

Outlook for Horizon 2

Nb. Where appropriate to do so, we have consolidated some of the consultations questions.

What trends or technology developments will shape the outlook over the next few years and what other strategic factors should Government be exploring for cyber security under Horizon 2?

The uptake, and increasing strategic importance of AI will have three significant implications for cyber security that will need to be accounted for under Horizon 2:

- **Changing threat landscape:** AI technologies can, and are, being used by cyber attackers to make some elements of cyber intrusion operations more effective and efficient, leading to an increase in frequency and intensity of cyber threats. As deepfake technologies improve and become more widespread in social engineering and digital identity attacks, investment in detection capabilities and secure, economy-wide digital identity programmes will be critical.
- **Evolving cyber defence capabilities:** Where cyber attackers have access to AI tools, so do cyber defenders. It is being used by the cyber industry to analyse large data sets at scale, support threat intelligence and mimic the behaviours of cyber attackers, so that organisations can understand and prepare for potential attacks. The Government should consider how it can encourage further R&D in this space, developing Australian AI-enabled cyber capabilities.
- **A need for safe and secure AI:** The Tech Council estimated that generative AI could contribute $115 billion annually to Australia's economy by 2030[1]. The widespread uptake and increasing reliance on AI warrants a proportionate regulatory response that establishes appropriate safeguards – not least because the growing incorporation of AI in Australia's technology base presents an increased attack surface for adversaries to exploit. This should ensure risks are mitigated, trust is built and, ultimately, Australia is able to benefit from the opportunities AI models present. In practice, we support previously consulted-on plans to develop a new AI Act – one that is risk-based, pro-innovation, and builds on existing ACSC guidance. At the same time, if the Government wants to ensure that Australian languages, religious outlooks,

[1] Generative AI could contribute $115 billion annually to Australia's economy by 2030 - Tech Council of Australia

values and cultural references are protected, while also minimising the risk of adopting biases seen elsewhere in the world, steps must be taken to develop Australian large language models, including by making Australian datasets more readily available for use in AI.

The transition to post-quantum cryptography (PQC) is also likely to be a defining factor in Australia's cyber security strategy over the next few years. We welcome the 2030 timeline set by ASD for High Assurance Cryptographic Equipment (HACE)[2], and recommend that a fuller roadmap is developed signalling to both public and private sector organisations what they need to achieve and by when. In addition, the Government should continue to work closely with the Five Eyes to consider where shared capabilities and standards can be developed, including a coordinated strategy on protecting satellite communications.

Collaborating across all levels of Australian Government

Are there initiatives or programs led by State or Territory governments you would like to see expanded or replicated across other levels of government?

While there no specific initiatives we would reference, on the subject of cross-government collaboration, intelligence sharing across State, Territory and Federal government (and government agencies) should be improved.

We also believe there needs to be greater consistency in the transparency, explainability risk management and supply chain standards applied across all levels of government where AI is being developed and used.

Monitoring progress in a changing world – a conceptual framework for evaluating cyber security outcomes

Does the high-level Model resonate and do you have any suggestions for its refinement? Can you suggest any existing or new ways to collect data and feedback to monitor these outcomes?

We welcome the holistic approach to evaluating the efficacy of policy interventions. The Government could utilise incident reporting data – recently centralised through the single reporting platform - to measure how policies impact cyber threats. This should be supplemented with annual surveys of Australian organisations to understand and measure the financial, organisational and personal impacts of cyber attacks, and how these change over time in response to government policies.

Shield 1: Strong businesses and citizens

What could government to do better target and consolidate its cyber awareness message? What programs or pilots have been successful in this context? What additional supports could be developed or scaled-up to address these issues in

[2] Guidelines for cryptography | Cyber.gov.au

partnership with both education stakeholders and those with technical cyber security expertise?

We agree that there needs to be a step change in citizens' cyber skills, empowering them to make informed decisions about the technology they use and take control of their cyber security. We also agree that promoting such skills can be best developed through schools, while also helping to create the next generation of cyber professionals.

With that in mind, we believe that 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. Teachers must also be regularly supported to understand new developments and how they should be reflected in the school curriculum.

At a higher education level, strict rules around how industry can engage students is hampering mentorship and lecturer opportunities that would help students to transition into the workforce. The Department of Home Affairs should work with the Department of Education to explore how existing requirements could be reformed to allow greater industry engagement.

Outside of formal education, a major cultural shift within company boards is needed, enhancing understanding of cyber security concepts across senior leadership so that they can take ownership for cyber risk in the same way that they own other core business risks.

How can Government encourage SMBs and NFPs to uptake existing cyber resources (i.e. Small Business Cyber Resilience Service, Cyber Wardens, ACNC guidance etc.)? How can industry at all levels and government work together to drive the uptake of cyber security actions by SMEs and the NFP sector to enhance our national cyber resilience? What existing or developing cyber security standards, could be used to assist cyber uplift for SMBs and NFP's? and NFP's? What are the unique challenges that NFP entities face for cyber security compared to the broader business sector and what interventions from government would have the most impact in the NFP sector?

The conundrum of addressing the cyber security risk to small and medium-sized businesses (SMBs) and non-for-profits (NFPs), without unfairly burdening them with costly requirements, remains a perennial challenge that has yet to be solved in a sustainable way. A 2023 ASIC survey found that small organisations consistently reported less mature cyber capabilities than their larger counterparts[3], not least because they "are regularly required to manage competing priorities with limited financial and human resources". For this reason, the use of regulatory levers to drive uptake of cyber security standards among SMBs and NFPs is likely to be disproportionate (unless the business is a critical supplier to critical infrastructure or government).

[3] Report REP 776 Spotlight on cyber: Findings and insights from the cyber pulse survey 2023

The launch of the Small Business Cyber Resilience Service is a welcome step, providing micro-businesses with somewhere to turn to in the event of a cyber attack. However, further work is needed to enhance SMB and NFP resilience upstream. In this regard, the most impactful (and proportionate) measures are likely to involve ensuring that the technology and services SMBs and NFPs rely on are secure-by-default and secure-by-design.

How well do you consider you understand the threat of ransomware, particularly for individuals and small entities? How is this threat evolving or changing? How could the government further support businesses and individuals to protect themselves from ransomware attacks?

It's worth noting that for smaller organisations ransomware incidents are more likely to pose an existential threat. A European Union survey of SMBs, for example, found that 57% said they would most likely become bankrupt or go out of business as a result of a cyber attack[4].

As larger organisations become more resilient to the level of sophistication seen in the most common ransomware actors, those same actors may continue to focus on smaller and less cyber mature organisations. These entities are less likely to have cyber insurance, and the impact of an attack more likely to lead to bankruptcy or permanent closure. This shift in targeting underscores the need for tailored support and intervention for small businesses and NFPs.

As noted above, the Small Business Cyber Resilience Service provides much needed incident response support to micro-businesses. The service could be expanded over time to:

- Provide subsidised incident response and advisory services to firms above the current 19 employee threshold;
- Proactively support SMBs and NFPs to adopt ACSC guidance;
- Fund awareness and education campaigns, targeting SMBs through national media and engagement structures like membership organisations, and running Joint Cyber Security Centre (JCSC) advisory sessions.

How can support services for victims of identity crime be designed to be more effective in the context of increasing demand?

It's critical that regulators continue to hold regulated businesses to account for any breaches of data protection and cyber security rules that have led to identity theft. This should include the breached organisations providing ongoing and proportionate support to identity theft victims for an extended period, with clear signposting to where victims can access help.

More broadly, efforts should focus on building resilience, including rolling out the secure Australian Government Digital ID and the deployment of behavioural insight experts to shift user behaviour, so that device security updates and other basic measures are further embedded in the nation's psyche as standard practice.

Shield 2: Safe technology

[4] SMEs Cybersecurity | ENISA

What are best practice examples internationally that Australia should consider for enhancing our secure technology standards and frameworks? In particular, what approach do you consider would work best for edge devices, CER and operational technology?

We believe there is scope to extend the Cyber Trust Mark to capture all digital products, requiring organisations in the public sector and critical infrastructure to only purchase products which meet this standard.

The piecemeal approach to technology regulation we have seen in the UK, for example, is leading to an unnecessarily complex web of compliance for businesses developing and selling products to navigate. In contrast, we recommend a widened Cyber Trust Mark from which requirements can be tailored to specific product classes and risk profiles, drawing on key international standards like ETSI 303 645 for smart devices and ISA/IEC 62443 for industrial automation and control systems.

For higher-risk products, manufacturers' and developers' compliance should be technically validated by independent third parties to ensure the requirements have been implemented correctly. This is in line with best practice across other sectors (e.g. smart metering) and will help to ensure a level playing field between those who are taking their security responsibilities seriously and those who may not be.

To support SMBs who supply digital products in adopting an expanded Cyber Trust Mark (CTM) or similar scheme, the government could offer financial incentives such as grants, tax rebates, or subsidised certification costs. Coupled with a national awareness campaign promoting certified secure products, these measures would help SMBs gain market visibility, build consumer trust, and contribute to raising cyber security standards across the broader economy.

How should the government work with you to support consumers and end-users to be more informed about cyber security in their products and protect themselves from cyber threats?

The ACSC should utilise the cyber industry as an amplifier of its guidance, utilising the network of organisations they support and promoting ACSC as a single authoritative source.

What additional guidance do you or your organisation need to manage foreign ownership, control or influence risks associated with technology vendors?

Where risks are present, particularly in sectors handling sensitive data or national security, the Australian government might partner with trusted AUKUS-aligned cybersecurity providers like NCC Group to deliver independent assurance. These providers can conduct rigorous assessments of technology vendors, validate security controls and help mitigate risks. For example, NCC Group is acting as a third-party security provider to independently

audit TikTok's European data controls and safeguards, monitor data flows, provide independent verification of security protocols, and report any incidents[5].

How could government better work with industry to understand data access and transfer across the economy to inform policies around secure data sharing and limit data exploitation from malicious actors? Boosting innovation and economic prosperity is enabled when data is shared with trust and not accessed exploited by malicious actors (e.g. IP theft). How does Government and Industry work together to achieve this aim in an evolving global threat environment?

Broadly speaking, we support the approach set out in the 2022 Australian Data Strategy, which focuses on data maturity, governance, and secure infrastructure.

What guidance can government provide to support the safe and responsible uptake of critical and emerging technologies? What do you consider to be the most serious national security risks presented by critical and emerging technologies, such as AI?

As outlined in more detail above, the increasing prevalence of AI presents two key cyber security risks, which require distinct responses:

1. **An increase in the frequency and intensity of cyber threats:** To counter this threat, the Government should work with industry and academia to develop (AI-enabled) countermeasures and defence capabilities. This could include the creation of challenge-led R&D funds.

2. **An increased attack surface for adversaries to exploit:** To address these (and other) risks, we support previously consulted-on plans to develop a new AI Act – one that is risk-based, pro-innovation, and builds on existing and new ACSC guidance.

The development and misuse of quantum technologies also present significant risks to the cyber security of communications and connected infrastructure. A detailed national PQC roadmap is needed, signalling to both public and private sector organisations what they need to achieve and by when. This should be accompanied by regularly updated ACSC guidance (including the Information Security Manual (ISM)). In addition, the Government should continue to work closely with the Five Eyes to consider where shared capabilities and standards can be developed, including a coordinated strategy on protecting satellite communications.

Shield 3: World-class threat sharing and blocking

What could government do to support and empower industry to take a more proactive cyber security posture to ensure the resilience of our cyber security ecosystem? What do you think Australia's proactive cyber security posture should look like for industry?

1. **Regulatory frameworks that reflect modern threats and critical systems**

[5] https://www.nccgroup.com/newsroom/ncc-group-signs-three-year-project-clover-contract-extension-with-tiktok/

SOCI provides a strong foundation for Australia critical infrastructure resilience. However, as new threats emerge, and sectors rise and fall in their 'criticality', it's important that the legal framework remains flexible and up to date. To that end, we strongly recommend:

- **Enhancing the Act's minimum security requirements over time**, with a greater focus on resilience and immediate steps to clarify and strengthen obligations related to supply chain, AI and PQC risks.
- **Reviewing regulated sectors** to reflect the inevitable evolution of what constitutes critical infrastructure and systems of national significance. Indeed, other jurisdictions – including the EU, UK and Singapore - are extending equivalent rules to critical suppliers, managed service providers and increasingly important industries like space.
- **Replicating the successes of the CORIE framework** across other key sectors, so that that organisations and regulators can benefit from the enhanced understanding of cyber threats that intelligence-led adversary emulation and simulation can bring.

2. **Cementing Australia's public-private partnership**

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 co-creation of capabilities, regular feedback mechanisms on key initiatives and guidance, and the rollout of two-way secondment schemes.

3. **Enhanced information sharing**

While recently enhanced reporting requirements will (rightly) help to build Government's understanding of the threat landscape, it's important that information sharing is approached as a two-way endeavour.

At present, reporting is often one-way, with only limited threat analysis shared with partners and the public. We welcome the Government's plans to enhance threat intelligence sharing with the private sector. This should be underpinned by efforts to cultivate a culture of trust and mutual learning. Greater awareness will lead to better understanding of cyber threats and will encourage the adoption of proactive activities.

4. **Investment in cyber defensive and offensive capabilities**

The last 18 months or so have been incredibly successful for law enforcement interventions and takedowns. We welcome the Government's global leadership in this area and request that this focus continues going forward.

5. **Enhanced SMB support**

As noted above, SMBs are far less likely to access to the expertise and resources needed to significantly enhance their cyber security posture. We would therefore support the expansion of the Small Business Cyber Resilience Service provides over time to:

- Provide subsidised incident response and advisory services to firms above the current 19 employee threshold;
- Proactively support SMBs and NFPs to adopt ACSC guidance;
- Fund awareness and education campaigns, targeting SMBs through national media and engagement structures like membership organisations, and running Joint Cyber Security Centre (JCSC) advisory sessions.

Does the government need to provide clarity on permissible and non-permissible Active Cyber Defence in the Australian context?

Yes. Legal clarity on what activities are deemed permissible and non-permissible, across both the private sector and the State, will not only help industry understand what they can and can't do, but could also act as a threat actor deterrent.

Alongside this, cyber security professionals undertaking permissible Active Cyber Defence activities must be able to access appropriate legal protections. NCC Group has been a longstanding campaigner for cybercrime laws to be updated so that they reflect modern and accepted industry techniques. For example, in the UK, we advocate for the inclusion of a principles-based defence in their Cybercrime Act 2001-equivalent – the Computer Misuse Act 1990[6]. While the legal frameworks do differ, both the Australian and UK laws criminalise unauthorised access of computers. The result is the same - some forms of legitimate security vulnerability research, threat intelligence and Active Cyber Defence activities are effectively criminalised in both jurisdictions. The Government should consider if similar legal reforms are required in Australia, as part of its work to explore legal safe harbours for vulnerability researchers.

How could government further support industry to block threats at scale?

We broadly support the government's approach to date, including its cooperation with critical infrastructure and reactive disruption activity, and advocate for more of the same.

How could the use of safe browsing and deceptive warning pages be amplified?

The use of safe browsing and deceptive warning pages could be amplified through a combination of technical integration, and policy support. Governments and industry bodies can encourage browser and communication technology companies to adopt standardised APIs that trigger warnings when users encounter known malicious or deceptive content. Additionally, regulatory frameworks can mandate the inclusion of safe browsing features in consumer-facing digital products.

[6] New Research: a proposal for a principles-based framework for the application of a statutory defence under a reformed Computer Misuse Act — CyberUp

What more is needed to support a thriving threat sharing ecosystem in Australia? Are there other low maturity sectors that would require ISACs, and what factors, if any, are holding back their creation? How can we better align and operationalise intelligence sharing for cyber security and scams prevention?

Multiple ISACs already exist; however, further work could be done to improve the quality and availability of sectoral and threat data to enrich predictive and automated response. We also see opportunity for ACSC to anonymise and disseminate threat information more widely, particularly with the new reporting requirements coming into effect.

Are the roles and responsibilities of government and industry clear for cyber security in a conflict or crisis scenario? What activities, such as cyber exercises, could Government undertake to make you feel better prepared to respond in a cyber conflict or crisis?

Tabletop exercises are being undertaken as part of SOCI Act and sector regulation compliance. The Gold Team exercise (tabletop) detailed in the Council of Financial Regulators CORIE framework provides structured guidance to ensure tabletop scenarios are informed by threat intelligence and focus on the organisation's most critical business services. This approach helps simulate realistic, targeted cyber threats and supports strategic decision-making during resilience testing. Consider adopting more formally under the SOCI Act the successes of the CORIE framework, so that that CI can benefit from the enhanced understanding of cyber threats that intelligence-led adversary emulation / simulation can bring.

Additionally, there is further scope for improvement when it comes to industry-government collaboration and joint tabletop exercises. Such initiatives will help to cement the roles and responsibilities of the affected parties in the event of a conflict or crisis.

How could government better incentivise businesses to adopt vulnerability disclosure policies (VDPs)? Does Australia need a vulnerability disclosure program to provide security researchers with a mechanism for safely reporting vulnerabilities?

To incentivise uptake of VDPs, we recommend requiring critical infrastructure, as a first step, to have one in place.

We support the Government's efforts to address the legal ambiguity faced by vulnerability security researchers. As noted above, we advocate for the inclusion of a principles-based defence in their Cybercrime Act 2001-equivalent – the Computer Misuse Act 1990[7]. Similar reforms could be appropriate in Australia, whereby cyber security professionals undertaking activities where authorisation is difficult or impossible to obtain can access a legal defence so long as they are able to evidence their adherence to the following principles:

- **Harm-benefit:** The (prospective) benefits of the act outweigh the (prospective) harms, including where action was necessary to prevent a greater harm.

[7] New Research: a proposal for a principles-based framework for the application of a statutory defence under a reformed Computer Misuse Act — CyberUp

- **Proportionality**: Reasonable steps were undertaken to minimise risks.
- **Intent**: The actor demonstrably acted in good faith, in an honest and sincere way.
- **Competence**: The actor is able to demonstrate their competence (authority and expertise) e.g. through qualification, certification or accreditation.

Shield 4: Protected critical infrastructure

How effective do you consider the SOCI Act at protecting Australia's critical infrastructure? Are the current obligations proportionate, well-understood, and enforceable?

SOCI provides a strong and largely proportionate foundation for Australia critical infrastructure resilience. However, as new threats emerge, and sectors rise and fall in their 'criticality', it's important that the legal framework remains flexible and up to date. To that end, we strongly recommend:

- **Enhancing the Act's minimum security requirements over time**, with a greater focus on resilience and immediate steps to clarify and strengthen obligations related to supply chain, AI and PQC risks.
- **Reviewing regulated sectors** to reflect the inevitable evolution of what constitutes critical infrastructure and systems of national significance. Indeed, other jurisdictions – including the EU, UK and Singapore - are extending equivalent rules to critical suppliers, managed service providers and increasingly important industries like space.
- **Replicating the successes of the CORIE framework** across other key sectors, so that that organisations and regulators can benefit from the enhanced understanding of cyber threats that intelligence-led adversary emulation and simulation can bring.

Are there significant cyber security risks that are not adequately addressed under the current framework?

Yes. Supply chain, AI and PQC risks are not adequately addressed.

There also needs to be greater alignment with 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[8] (APRA), have updated their guidelines to ensure critical infrastructure providers 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.

Is the regulatory burden on industry proportionate to the risk and outcomes being sought?

[8] Prudential Standard CPS 230 Operational Risk Management - clean

Broadly speaking, yes. But, as noted above, the legal framework will need updating to reflect evolving threats and the changing criticality of sectors. This should be supported by horizon scanning, consultation with industry partners and regular audits.

What support would assist critical infrastructure owners and operators to mature their cyber and operational resilience practices? What role should government play in enabling uplift, including through tools, guidance or incentives?

It's critical that Government get the right balance between incentives (i.e. carrots) and regulatory consequences (i.e. sticks).

On the one hand, the Critical Infrastructure Security Centre (CISC) must be equipped with the skills, capabilities and resources necessary to effectively enforce the SOCI regime. On the other hand, overreliance on the 'stick' could create a culture of fear and discourage early engagement and reporting. The Government must also focus efforts on building a culture of trust, mutual learning and support.

How can the Australian Government support private sector partners to better engage with government security requirements, including certifications and technical controls?

The Government should utilise procurement frameworks to encourage uptake of security requirements.

Shield 5: Sovereign capabilities

What role should government play in supporting the development and growth of Australia's cyber workforce? What initiatives, pilots or policy ideas do you think would best support industry to grow?

The development and growth of the cyber workforce is closely linked to the upskilling of the broader population's cyber literacy skills. The Government can play a role setting a national cyber skills strategy that maps what cyber skills the nation needs and charts a plan of how we get there. Specific interventions should include:

- Reviewing rules around how industry can engage students at the higher education level, which is currently hampering mentorship and guest lecturer opportunities that would help students to transition into the workforce.
- 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. Teachers must also be regularly supported to understand new developments and how they should be reflected in the school curriculum.
- Starting cyber education and awareness in early school years.

How can industry, academia, think tanks and government best work together to set research priorities and drive innovation to further our strategic, economic and community interests and achieve our common goals? How can government and academia enhance its partnership and promote stronger people-to-people links and collaboration on research and policy development activities?

We support a 'whole of society' approach to tackling future challenges and developing new technologies. Joint councils and advisory groups can help to break down the barriers between industry, government and academia; however, many such structures already exist and often are either duplicative in their work or lack clarity on what their setting out to achieve. We recommend that the Government undertake a review of existing institutions and advisory bodies that exist to enable innovation in cyber security, digital resilience and the wider technology landscape, before considering what long-term mechanisms should be established to avoid siloed working and enable better collaboration.

How would we best identify and prioritise sovereign capabilities for growth and development across government and industry?

There needs to be strong alignment with Australia's broader national security and technology strategy, as well as regular in-built reviews (in consultation with industry) to assess whether chosen sovereign capabilities are still applicable.

More broadly, and building on the work of partnerships like AUKUS, the Government should consider what its approach to 'shared sovereignty' is. Acknowledging that onshoring everything is likely to be impossible, the Government should work with Five Eye allies on the development of key capabilities.

What are the areas of most concern for ICT concentration and what do you consider would be most effective as mitigation strategies to explore?

One effective mitigation strategy is to adopt a 'Resilience by Design' approach, assuming supplier failure, regardless of their risk profile, and promoting the use of practical and cost-effective resilience solutions such as back-ups and escrow agreements. Such an approach can build businesses' confidence in the adoption of new technologies by implementing what are effectively technical insurance policies and safeguarding the long-term availability of business-critical systems and intellectual property.

Shield 6: Strong region and global leadership

Do you view attributions, advisories and sanctions effective tools for countering growing malicious cyber activity? What other tools of cyber diplomacy and deterrence would you like to see Australia consider for development and use to effectively combat these threats in Horizon 2?

Attributions, advisories and sanctions remain core statecraft tools that the Government should continue to invest in. Indeed, Australia has been a global leader in this area over the last few years. Going forward, the Justice Department, Law Enforcement and the Treasury

should double down to impose arrest warrants, extraditions and sanctions. Penalties and sanctions should be extended to organisations helping groups launder illicit funds.

Globally, Australia should continue to utilise successful partnerships like the Five Eyes alliance, AUKUS and the International Counter Ransomware Initiative (CRI).

In which forums and on which issues would you like Australia to focus efforts to shape rules, norms and standards in line with its interests most effectively in Horizon 2?

We recommend that the Government encourages Australian industry experts to take a leading role in international industry bodies such as CREST, ISACA 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.

What regulatory frameworks or requirements should be prioritised for consideration as part of Australia's efforts on international cyber regulatory alignment?

We strongly support Australia's efforts to align cyber regulations globally. As the consultation document points to, most leading economies have or are adopting very similar organisational and product-based regulations to Australia. Alignment will reduce regulatory burdens, without compromising security outcomes.

In terms of specific frameworks, the following should be prioritised:

- **Critical infrastructure (SOCI equivalents):** EU's NIS2, the UK's current NIS regulations, Cyber Security and Resilience Bill, Telecoms Security Act, US sectoral regulations, and Singapore's Cybersecurity Act.
- **Financial services:** EU's DORA.
- **Digital products (Cyber Security Act equivalents):** UK's Product Security and Telecoms Infrastructure (PSTI) Act.