Deloitte.

2023 – 2030 Australian Cyber Security Strategy Discussion Paper

Submission

Foreword

Deloitte's Submission to the *2023 – 2030 Australian Cyber Security Strategy* Discussion Paper

I am pleased to enclose Deloitte's submission to the *2023 – 2030 Australian Cyber Security Strategy* ('the Strategy') Discussion Paper to the Expert Advisory Board.

As the Discussion Paper notes, Australia's key cyber security objective is the integrated whole-of-nation endeavour required to lift and sustain our cyber resilience through to 2030.

Both the Discussion Paper and the Australian Cyber Security Centre's *Annual Cyber Threat Report 2021-22* highlight the scale of malicious activity in Australia — one incident is reported on average every 7 minutes. As Australia has experienced with the recent high-profile and significant data-breaches, the impact of these activities is widespread and indiscriminate; they disproportionately affect the most vulnerable in society — the small-medium enterprises and individuals least able to protect themselves. Equally worrying is the potential effects of cyber attacks on Australian Critical Infrastructure, which undermines both public trust and our way of life.

Deloitte submits that a key outcome for the Strategy is to enable Australia to generate the scale, speed and 'tempo' to prevent, mitigate and respond to threats-at-scale to 2030 and beyond. This will require us as a nation to come together to collaborate in unprecedented ways, leverage collective skills and resources deliberately and efficiently, and create effective synergies in many of the following areas:

- Cyber threat sharing and blocking at-scale
- Cyber collaboration through sectoral Information Sharing and Analysis Centres (ISACs)
- Government cyber uplift and leading by example
- Our national cyber workforce
- Evolving cyber security technologies
- Supporting international cyber resilience.

Our submission examines these areas and offers actionable recommendations for the Expert Advisory Board's consideration. As well as speed and scale, we emphasise the principles of co-design, incentivisation, collaboration and interoperability throughout our submission.

Taken as a whole, we believe our recommendations help support the creation of a national cyber security ecosystem that is greater than the sum of its parts. To become the most cyber-secure nation in the world by 2030, Australia needs to establish the necessary momentum, structures and coordination to defeat cyber threats-at-scale. We look forward to continuing to support this significant national endeavour.

Adam Powick
Chief Executive Officer, Deloitte Australia

14 April 2023

Contents

1. Executive Summary

Deloitte's Recommendations

Deloitte's submission to the Expert Advisory Board has been grouped within the following themes:

- Collaborating on cyber threats
- Government as a cyber role model
- Growing Australia's cyber workforce
- Cyber security technologies
- Supporting international cyber resilience.

This recognises both the cross-functional nature of the questions posed in the Discussion Paper, and the multifaceted challenges of cyber security.

Our approach has been to focus on what we view as the fundamental challenge for Australia in becoming the most cyber-secure nation by 2030 — how we as a country can generate 'the scale to meet the scale' of global cyber threats. Importantly, we do not just want Australia to meet the challenge; our nation has to create the tempo and asymmetry to prevent and defeat evolving threats.

In providing recommendations to the Board, we note our intent for many of our recommendations to both address specific Discussion Paper questions, and work in concert to achieve national-level synergies. We thank the Expert Advisory Board and the Department of Home Affairs for the opportunity to contribute to this highly-significant national strategy.

Recommendations

1. Government applies a **whole-of-lifecycle co-design approach** to collaborative or cross-sectoral cyber initiatives.

2. Government **invests in, seeds and fosters threat-blocking programs** and consortiums, including developing appropriate **interoperability and integration nationally** through CTIS and other threat-sharing mechanisms.

3. Government invests in and promotes **sectoral-based cyber collaboration bodies based on international best practice.** This may include evolving existing mechanisms (such as the TISN) to support industries leading and implementing their own **Australian-based sectoral ISACs.**

4. Government invests in **mechanisms that encourage effective sharing of lessons-learnt post-incident**, including through ISACs and other sectoral industry intermediaries.

5. The development of a **joint Commonwealth funding model** that enables government department and agencies to implement repeatable cyber uplift programs.

6. Government cyber security investments are measured as a percentage of overall organisational spend that supports **increased transparency and benchmarking**.

7. A Federal Government ISAC (or similar model) is established to **generate repeatable and scalable models for whole-of-government cyber uplift**, and supports the Federal Government in leading by example nationally.

8. The development of government investment mechanisms (directly or indirectly, including through tax breaks) in **scalable public-private partnerships models** for cyber workforce training.

9. Government investigates opportunities to **integrate cyber security into broader curricula**, including in K-12, and in fields like business and engineering.

10. A co-design process is implemented with government and industry to **review and uplift both the TDIF and Gatekeeper** standards, including establishing a joint public-private expert governance committee.

11. The development of a **national at-scale approach to Privacy Enhancing Technologies** by Government, including a national strategy, incentives for adoption, and an expert governance committee.

12. An **enhanced risk assessment approach is considered for CIRMP** that enhances consistency of critical dependency mapping for key organisational processes. This should include mechanisms to train and certify of relevant risk practitioners.

13. To **scale how Australia collaborates on regional cyber resilience**, cyber security should be considered for integration in all relevant Australian Government regional and bilateral resilience and development programs.

14. Additional to Recommendation 3, Government considers the establishment of a specific **Australian Defence Industrial Base ISAC** to support AUKUS and broader Defence capability programs.

15. Government also considers the role of broader sectoral ISACs in supporting **Track II** and **regional cyber resilience** programs.

2. Collaborating on Cyber Threats

Discussion Paper Questions 7, 10, 13 & 14

Trust is key to collaboration

2.1 There are clear benefits from collaboration in cyberspace. Stakeholders from across the Australian economy manage information that, in aggregate, can prevent cyber threats from spreading across supply chains, industries or between Critical Infrastructure (CI) sectors. But, collaboration is only possible where there is trust and trusted mechanisms. Many benefits of cyber collaboration are unrealised due to the lack of both trusted mechanisms to collaborate and a corresponding culture of trust. The Australian government has to continue its convening role in bringing sectors together, and build trust and trusted mechanisms into the design and operation of national cyber initiatives, including on sectoral threat collaboration.

2.2 Australia already has strong foundations for a trusted collaborative national ecosystem. For example, the success of the Australian Cyber Security Centre's (ACSC) Cyber Threat Intelligence Sharing (CTIS) service presents a clear, repeatable model for the use of co-design concepts to embed trust and collaboration into other national cyber initiatives.

Case Study – ACSC's CTIS Co-Design

The Australian Cyber Security Centre's (ACSC) CTIS platform went live in late 2021. The CTIS service is a national community of cross-sectoral organisations that share threat intelligence bi-directionally, at machine speed.

The initial implementation of the CTIS system was the result of a series of co-design activities held with key participants across government, CI operators and industry (including Deloitte). This spirit of co-design continues today, with the CTIS community actively contributing to technical and operational decisions at regular Technical Advisory Work Group sessions.

2.3 These tested co-design models provide government with the ability to win the hearts and minds of prospective industry collaborators by listening and providing a deeper understanding of what works for both government and industry. This deeper understanding helps to bring out the best of our collective abilities, and fosters a sense of accountability and public-private partnership towards shared goals — creating sustainability in our national cyber initiatives. Importantly, co-design best practice requires application throughout a cyber program's lifecycle — at design, inception, enhancements and transition.

Recommendation 1: Government applies a whole-of-lifecycle co-design approach to collaborative or cross-sectoral cyber initiatives.

The challenges of speed and scale

2.4 Scale and speed are defining trends in cyber and our broader digital economy – they can provide vast economic benefits but also intensify malicious activity. To protect Australia's national interests online, governments need to invest in sharing and blocking capabilities that keep pace with the rapidly-evolving global cyber threat landscape. We believe that the key to overcoming this scale and speed asymmetry is building a national ecosystem that capitalises and synergises the strengths of both industry and government, while mitigating weaknesses.

2.5 Effective threat blocking initiatives at scale should, for example, aim to minimise low-level breaches for all participants and enable organisations to focus on novel and unique threats. The Strategy provides an opportunity for government to invest in and expand threat blocking programs at-scale that help protect those that cannot protect themselves.

2.6 Industry-led consortiums represent a strong model for threat blocking. To evolve and meet the challenges of speed and scale, these initiatives need to interoperate in a common national ecosystem. This is where the Australian government is well-placed to lean in and cohere existing programs and investments into interoperable ecosystems that work at scale through the most able organisations to protect the most vulnerable. There is a natural and logical connective tissue that should be established between real-time threat sharing ecosystems, such as the ACSC's CTIS service, and information-sharing conducted by 'intelligence-hungry' threat blocking consortiums.

2.7 For example, many Commonwealth, State and Territory government entities are protected by the ACSC's Australian Protective Domain Name Service (AUPDNS) that blocks connections to 'bad' domains or malicious actors. Ongoing integration of CTIS intelligence feeds into AUPDNS evolves threat-blocking at scale, and establishes the technical foundations for interoperability for threat-blocking programs. We believe this is an exemplar pilot model for how the Australian government can consider generating speed and scale through 1) automated threat sharing and blocking programs, and 2) sustainable and scalable collaboration between government and industry.

Recommendation 2: Government invests in, seeds and fosters threat-blocking programs and consortiums, including developing appropriate interoperability and integration nationally through CTIS and other threat-sharing mechanisms.

2. Collaborating on Cyber Threats

Discussion Paper Questions 7, 10, 13 & 14

2.8 The need for scale and speed also extends beyond threat sharing and blocking. Automated cyber threat intelligence is ineffective without rich contextualisation. While government-funded initiatives like CTIS and the Trusted Information Sharing Network (TISN) have laid strong foundations, there remains significant demand and potential growth opportunities for rich, sector-specific threat sharing and collaboration.

2.9 Industry-led initiatives like Information Sharing and Analysis Centres (ISACs) have established a strong track record internationally for sector-based sharing and collaboration. ISACs incentivise organisations to collectively manage the challenges of speed and scale by providing safe spaces for industry peers to share non-commercial knowledge among a network of trusted partners. This contrasts with merely reporting information to satisfy compliance and/or regulatory requirements.

2.10 As industry-led bodies, ISACs can deliver scaled-services and gain rich sectoral insights that government cannot achieve alone. ISACs represent a compelling 'next generation' of cyber security resilience in Australia, with the potential to augment existing sectoral initiatives (e.g. TISN) into industry-led 'spokes' of government-led 'hub' ecosystems (e.g. CTIS). The deep sectoral focus helps operationalise, scale and synergise the efficacy of automated cyber threat intelligence sharing. The buying power of sectoral ISACs also allow members to access a scalable catalogue of managed services more readily and efficiently.

2.11 These sectoral collaboration initiatives ultimately add to total organisational resilience, rather than unintentionally stripping organisations of their limited skilled resources. Internationally, ISACs serve to rationalise aspects of the 'war for cyber talent'. They support the collectivisation of resources to combat shared challenges, creating and enabling employment mobility that benefits all member organisations.

Case Study – Information Sharing and Analysis Centres (ISACs)

Information Sharing and Analysis Centres (ISACs) are communities that help sectors work together to combat shared threats. ISACs were first founded in the United States by a Presidential Directive in 1998 to support collaboration and sharing between Critical Infrastructure operators.

ISACs are now tried and tested, with similar models being adopted in the EU, Canada, Japan, and Taiwan. While successful ISAC models are defined based on the needs of the industry sector, ISAC services generally conform to four broad capability categories: threat intelligence sharing, member-led sector collaboration and communication, reporting and compliance, and cyber support services. The case for ISACs as the next generation of security resilience for Australian industry has been detailed in a recent Deloitte research paper, accessible here.

2.12 Importantly, best-practice ISACs are member-led bodies, built on the principle that organisations are stronger on security when given the opportunity to lead themselves. This represents a fundamentally new model for Australia, providing industry leaders with clear mechanisms to exercise leadership for the benefit of their industry, broader supply chains and the economy as a whole. Unlike closed groups (that are currently ad-hoc CISO or vendor-led), member-led ISACs enable broader industry leader-level collaboration to drive the strategic changes required to incorporate systemic cyber risks into a modernised view of corporate responsibility and ESG. This also enables a top-down transformational approach required within organisations to change the way they collaborate with others – this is rarely successful bottom-up, not least due to the investments required.

Recommendation 3: Government invests in and promotes sectoral-based cyber collaboration bodies based on international best practice. This may include evolving existing mechanisms (such as the TISN) to support industries leading and implementing their own Australian-based sectoral ISACs.

Responding to major cyber incidents

2.13 Australian organisations are expected to navigate an increasingly complex web of obligations and reporting as they respond to threats and incidents. While a single government reporting portal has already been proposed as a solution by the Productivity Commission and other bodies, consolidation alone will not resolve this complexity. The needs of different sectoral regulators will continue to drive requirements for tailored reporting models. Consolidation efforts should be supported in parallel by the consideration of legal safe harbours as well sectoral intermediaries (see below) that support more open, timely and effective reporting.

2.14 Sectoral intermediaries such ISACs can sit in the middle of this complex reporting web, facilitating faster and more consistent engagement between relevant stakeholders. In addition to maintaining a library of sector-specific templates and guidance, ISACs can play an important role in all-hazards crisis coordination and communications, and national preparedness exercises. They can support sovereign emergency management capabilities, maintaining distribution lists and playbooks informed by relevant, up-to-date industry information and regulatory requirements.

2.15 ISACs and other sectoral intermediaries such as cyber security responders and advisories provide an important function in the incident-response ecosystem by supporting effective sharing of the aggregated lessons-learnt following major incidents. Although the Strategy will consider the current legal and policy blockers on post-incident information sharing, we posit that it is not just about the ability to share, it is how to effectively share with context.

Recommendation 4: Government invests in mechanisms that encourage effective sharing of lessons-learnt post-incident, including through ISACs and other sectoral industry intermediaries.

3. Government as a Cyber Role Model

Discussion Paper Question 6

Investing in Repeatable & Scalable Models

3.1 The development of a national strategy to 2030 provides significant opportunities for the Australian Government to lead by example on cyber uplift. The Protective Security Policy Framework (PSPF) *Assessment Report 2021-22* states that, on information security outcomes, only 18% of Non-corporate Commonwealth Entities (NCEs) self-report as being at 'managing' or higher maturity. This suggests opportunities to substantially invest in current uplift programs to improve their overall efficacy.

3.2 Specifically, in designing uplift programs, government departments and agencies should invest in repeatable models that create cost-efficiencies, and which promote shareability and interoperability across the Commonwealth, States and Territories, and with international partners. This supports uplift at-scale and consistency across the whole-of-government.

3.3 A key lever for promoting investment in repeatable models is funding. Investments in cyber security vary across departments and agencies, and are often driven by compliance activities and incident response. Even where services are provided for free, such as with the ACSC's, smaller government entities may still lack the financial resources and skills required for implementation.

3.4 Developing a model for joint Commonwealth funding for common cyber uplifts programs may help to both support consistent long-term funding for departments and agencies, and/or incentivise additional investments above compliance requirements. Importantly, joint funding for common cyber security programs also encourages repeatable government models for broader uplift.

This supports Commonwealth cyber security at-scale, particularly with interoperable threat-sharing and blocking services.

Recommendation 5: The development of a joint Commonwealth funding model that enables government department and agencies to implement repeatable cyber uplift programs.

3.5 This proposed model for joint funding, and its distribution, can be informed through increased transparency on how departments and agencies invest in information security. This could include annual measurement of cyber security spend as a percentage of overall organisational budgets. This also facilitates investment benchmarking against industry frameworks.

Recommendation 6: Government cyber security investments are measured as a percentage of overall organisational spend that supports increased transparency and benchmarking.

3.6 Machinery of Government (MoG) changes present a unique challenge for departments and agencies. Many existing government IT systems and technologies are not scalable or flexible enough to support frequent organisational changes. MoG changes often create cyber vulnerabilities. Repeatable and scalable models support the relevancy and continuity of government cyber uplift programs during these periods.

Cohering accountability and investments

3.7 Major government IT projects benefit from single points of ownership and authority. Yet, whole-of-government cyber uplift programs are often subject to competing priorities between departments and agencies.

This can lead to scope changes and implementation challenges. The dedicated focus of a Coordinator for Cyber Security, supported by a National Office for Cyber Security, is an opportunity for the Commonwealth Government to cohere ownership, accountability and execution of whole-of-government cyber uplift programs.

3.8 Earlier, we outlined the benefits of and our recommendations on ISACs. In the context of repeatable models, investing in a federal government ISAC-like model will help develop cross-agency collaboration and maturity that enable scalability with cyber uplift programs and frameworks, particularly if co-designed with both government and industry stakeholders. Beneficiaries include less-resourced agencies, who could more easily collaborate and implement open-source and other readily available cyber security services, including those provided by the ACSC.

3.9 A federal government ISAC also pools Commonwealth procurement power for both managed services (such as commercial threat intelligence feeds, managed security operations and attack surface management), and workforce training and uplift. Given the unique sensitivities involved with government information security, a cohesive ISAC-like structure also integrates national security agencies' support and collaboration more readily, particularly during major incidents. Importantly, a federal government ISAC model also allows the Commonwealth to definitively lead by example on threat sharing and collaboration across States and Territories, and with CI entities and industry.

Recommendation 7: A Federal Government ISAC (or similar model) is established to generate repeatable and scalable models for whole-of-government cyber uplift, and supports the Federal Government in leading by example nationally.

4. Growing Australia's Cyber Workforce

Discussion Paper Questions 11 & 12

Investing in Public Private Partnerships

4.1 Current market models have not delivered Australia's cyber workforce requirements. Organisations are often unable to hire skilled cyber professionals — ongoing access to talent and capabilities are usually significant obstacles to cyber uplift. To sustainably grow Australia's cyber workforce to meet our challenges to 2030 and beyond, the nation cannot continue to rely on the current status-quo of specialised courses and micro-credentialing. International research and benchmarking suggest many benefits can be achieved through a strong work-based learning system, which strikes a balance between ab-initio courses, tertiary education and on-the-job experience.

4.2 Government has a deliberate role to play in transforming how it collaborates with academia and industry to achieve systemic and sustainable change to Australia's cyber workforce development. This requires a dedicated focus on public-private partnerships that enable appropriate on-the-job training and which allow the nation's workforce pipeline to scale quickly.

Case Study – Deloitte Cyber Academy

Deloitte has collaborated with universities, TAFEs, industry and government to develop a an earn-as-you-learn cyber apprenticeship program. Inspired by successful international models, the Deloitte Cyber Academy provides a work-integrated learning model where students study for a Degree and Diploma whilst working at an employer organisation.

The model is designed to teach students the best technical, academic and human cyber skills, while simultaneously providing direct support to industry partners by helping them foster and grow their cyber workforce 'in-flight'.

Further information can be found here.

Industry Collaboration on Sector-Specific Cyber Resilience Challenges

4.3 Cyber skills are often niche and fall short of sector-specific demands. This has resulted in a highly competitive skills environment, in which well-resourced sectors and organisations can attract the most cyber talent — leading to shortages in other equally vulnerable parts of the Australian economy.

4.4 Sector-focused bodies like ISACs can help rebalance this equation. ISACs internationally have helped to identify skill deficiencies in a sector, and facilitate training, resource sharing, and procurement power to close these gaps. To scale and meet our workforce challenge, Australia will need to broaden how it searches for and acquires talent. Identifying traits required for cyber skills and roles, beyond traditional qualifications, as well as roles that work around people's unique circumstances is key to closing the talent gap, while also supporting workforce resilience through diversity.

4.5 Organisations and industries that do not have the same financial means or capability as others can struggle to attract and retain talent. Yet, it is arguably more important for these entities to adequately build their workforce to respond to increased cyber risk. There are opportunities here for government to consider various policy and fiscal levers to alleviate these pressures and incentivise the more effective use of existing cyber resources.

Managed services as a workforce enabler

Not all organisations have the skilled resources or capacity to perform critical cyber tasks in-house like detect and response, threat hunting and open source intelligence analysis. Managed services, delivered either by industry and government, are critical to unlocking efficiencies in resource-constrained cyber workforces.

Deloitte has observed among our own clients that the automation of managed services at-scale helps organisations focus and channel valuable cyber resources into higher priority tasks. For example, the use of Attack Surface Management technologies to automate asset discovery, review and remediation continuously frees up workforce capacity for 'higher-value' prevention, response and threat collaboration activities.

Recommendation 8: The development of government investment mechanisms (directly or indirectly, including through tax breaks) in scalable public-private partnerships models for cyber workforce training.

4.6 These models in Recommendation 8 should emphasise 1) on-the-job training and placements, 2) non-traditional cyber recruitment (e.g. lateral vs ab-initio skilled workers), and 3) preferential support for small-medium enterprises and critical industries to both recruit skilled cyber talent, and to access managed services such as threat blocking.

Long Term Curriculum View

4.7 Sustainably growing the Australian cyber professional pool requires a long-term curriculum planning approach. Integrating cyber throughout the broader education life-cycle, as opposed to it being a standalone tertiary discipline, will support broader cyber hygiene awareness across the nation and contribute to a healthier pipeline of future cyber-proficient professionals.

Recommendation 9. Government investigates opportunities to integrate cyber security into broader curricula, including in K-12, and in fields like business and engineering.

5. Cyber Security Technologies

Discussion Paper Questions 16, 17 & 19

Evolving the Digital Identity Ecosystem

5.1 The seismic shift in digital services requires an equivalent rethink on how digital identity serves as the foundation of the digital economy. Continued large-scale data breaches show that knowledge based methods of enrolling or authenticating users (passwords, Q&A) cannot reliably assure identity. Digital services that rely on the aggregation of Personally Identifiable Information (PII) attract identity fraud and cybercrime at-scale.

5.2 The Commonwealth's Trusted Digital Identity Framework (TDIF) serves as a good national foundation that has attracted significant interest across both government and private sector organisations. However, we recommend it evolve to consider:

- Real time, risk based monitoring of digital identity fraud
- How to securely leverage biometric validation as the default for identity proofing and digital services access, for any service that provides access to personal or sensitive information.
- How the TDIF can be extended to accommodate newer technologies such as verifiable credentials — or self sovereign identities (SSI) aligned to a trusted source — that put the user in control of their data, driving better privacy outcomes.

5.3 The Commonwealth's Gatekeeper Public Key Infrastructure (PKI) standard is a mature standard that has protected the Commonwealth's cryptographic authentication infrastructure for over 20 years. Private sector infrastructures have also been accredited under Gatekeeper. This standard remains important and should be maintained. However, we recommend it also evolves to consider:

- Specific rules for cryptographic means to protect Operational Technology (OT) and CI infrastructure.
- Mandating mutual PKI authentication for identity assurance.
- Accommodation of quantum computing developments to ensure the continued efficacy of supported algorithms.

5.4 The longevity of Gatekeeper has been a result of the original co-design and oversight by the Gatekeeper Policy and Governance Committee (GPGC); a committee of PKI specialists from government and industry. We recommend that this GPGC or similar body be reconvened. The TDIF would also benefit from a similar policy governance committee with specialist representation.

Recommendation 10: A co-design process is implemented with government and industry to review and uplift both the TDIF and Gatekeeper standards, including establishing a joint public-private expert governance committee.

Privacy Enhancing Technologies

5.5 Data privacy, identity and sharing are at the heart of many of Australia's current cyber challenges. Customers are concerned about PII protection at rest, in-transit and during processing, including by third parties. The Strategy provides opportunities for Australia to consider the adoption of Privacy Enhancing Technologies (PETs) at scale. The key goal of PETs is to allow government and businesses to extract value from data without exposing the data itself. The Strategy also provides Australia with an opportunity to keep pace with its international partners who are developing national strategies and policy initiatives around PETs.

Recommendation 11: The development of a national at-scale approach to Privacy Enhancing Technologies by Government, including a national strategy, incentives for adoption, and an expert governance committee.

Operational Technologies

5.6 It would be remiss to lose focus on the importance of OT when discussing cyber security technologies. OT systems are core to monitoring and control of industrial processes that underpin CI. OT systems often have a long in-service life (some exceeding 30 years), very high uptime requirements and are integral to core safety functions. OT systems are often based on dated technology that constrain the retrofitting of modern cyber controls, such as complex passwords. There are challenges in retaining sufficient workforce knowledge to recover or rebuild OT systems after critical incidents.

5.7 OT systems have historically been protected by isolation (i.e. 'air-gaps') as the main control, but this model is under pressure as more mainstream technologies (e.g. IP networking) and industrial Internet of Things (IoT) are adopted. The OT supply-chain presents key risks in terms of underlying hardware and software supply. In Australia, many systems have third-party support agreements with offshore vendors connecting to core systems to diagnose and support.

5.8 The current CI Risk Management Program (CIRMP) requirements can sometimes result in disjointed organisational analysis of the four 'hazard domains' of cyber, personnel, supply chain and physical. Many CI entities need support in modelling blended attack paths, such as those used by sophisticated threat actors executing supply chain attacks; these forms of 'sovereign risk' are often not adequately explored. Effective OT security requires a deep analysis of specific risks and attack paths to critical processes, including key upstream dependencies like OT, IT, suppliers and people. The US Department of Energy's Consequence-Driven, Cyber-Informed Engineering methodology (from Idaho National Labs) could provide a basis for this enhanced methodology.

Recommendation 12: An enhanced risk assessment approach is considered for CIRMP that enhances consistency of critical dependency mapping for key organisational processes. This should include mechanisms to train and certify of relevant risk practitioners.

6. Supporting International Cyber Resilience

Discussion Paper Questions 3, 4 & 5

Enhancing existing International Partnership Frameworks

6.1 Australia's many existing international partnership frameworks already support pillars for cyber collaboration, such as in the Association of South East Asian Nations (ASEAN) - Australia Comprehensive Strategic Partnership, Quad, and Pacific Islands Forum (including through Australia's Cyber and Critical Technology Cooperation Program (CCTCP)). This Strategy provides opportunities to enhance existing frameworks to build regional cyber resilience to 2030 and beyond.

6.2 The often-indiscriminate nature of malicious cyber activity, especially against CI, has the greatest effect on the most vulnerable groups. This is true both in Australia and in many regional countries, e.g. attacks on financial services in a country with a predominate cash economy. Increasingly, cyber security is not a distinct pillar for cooperation, but an area that pervades all aspects of development as economies are increasingly digitised. This trend influences how Australia should consider regional resiliency and development programs – cyber security should no longer be confined to a cyber cooperation pillar.

Recommendation 13: To scale how Australia collaborates on regional cyber resilience, cyber security should be considered for integration in all relevant Australian Government regional and bilateral resilience and development programs.

6.3 Although there is rightly an emphasis on supporting regional partners in incident response, the scale of malicious cyber activity requires Australia's support on regional cyber development to increasingly focus on preventative measures. Yet, prevention in an Australian context may not be applicable in an ASEAN or Pacific Islands country context.

6.4 There are many lessons learnt from Australia's diplomatic efforts regionally on complex issues such as climate change and counter-terrorism. What is clear from Deloitte's own experience when working with regional cyber security partners and clients is that contextualisation is critical – it is often not even about a lower cyber maturity, but the appropriate social and cultural context for cyber security.

Enhancing Industrial Base Interoperability

6.5 The recent development of the AUKUS partnership emphasises international cyber collaboration; both in terms of emerging technology collaboration in 'Pillar Two', but also in terms of supply-chain assurance that supports and protects allied Defence Industrial Base interoperability.

6.6 Deloitte's position is that cyber security underpins Australia's industrial base interoperability with international partners. Like workforce considerations, cyber security fundamentally enables AUKUS and other allied industry programs. Importantly, a sectoral approach to cyber security will help protect Small-Medium Enterprises (SMEs) that form critical parts of Australia's long-term sovereign Defence capability. This includes facilitating deeper cyber and all-hazards collaboration for Australia's supply chains, both internationally and with the Australian Government.

6.7 The benefits of ISACs were explored earlier in this submission. As an international benchmark, the US National Defense ISAC has been operating since 2017. A similar body for Australia provides government and the Australian Defence Industrial Base a mechanism to 1) benchmark its level of industry cyber collaboration, 2) interoperate and share cyber threat intelligence both domestically and with international partners, 3) support local and global supply chain assurance, and 4) enhance all-hazards and cyber security for Australia's SMEs.

Recommendation 14: Additional to Recommendation 3, Government considers the establishment of a specific Australian Defence Industrial Base ISAC to support AUKUS and broader Defence capability programs.

The role of industry

6.8 More broadly, Australian ISACs can also support: 1) greater international supply-chain assurance through common standards and threat collaboration, 2) unique sectoral perspectives on Australia and regional specific cyber threats, 3) enhancing Australia's position as a technology and cyber leader through cyber standards setting (which helps also to support regional resilience), and 4) the ability to scale industry's ability to support Track II diplomacy efforts on cyber.

6.9 This may be especially useful in terms of regional incident response. In practice, regional countries may raise sensitivities or even challenge any Australian government support to their domestic cyber incidents - industry can often act faster, and as a neutral broker, to support major incidents.

Recommendation 15. Government also considers the role of broader sectoral ISACs in supporting Track II and regional cyber resilience programs.

Deloitte.

Contacts

Ian Blatchford

National Cyber Leader
+61 2 9322 5735
iblatchford@deloitte.com.au

Rachelle Koster

Partner – Cyber
+61 421 051 630
rkoster@deloitte.com.au

Rob Parker

Partner – Cyber
+61 423 213 112
robparker@deloitte.com.au

Sean Choi

Principal – Cyber
+61 481 095 005
seanchoi@deloitte.com.au