AISA Australian Information Security Association

2023-2030 Australian Cyber Security Strategy Horizon 2 Response

Table of Contents

Foreword

AISA is pleased to provide this response to the request for consultation on developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy. Our submission covers questions asked in the consultation paper, incorporating valuable insights from our diverse membership, community, and the Executive Advisory Board for Cyber (EABC) that have been collected over the month the paper was open.

We remain dedicated to ensuring our members and stakeholders are engaged in the consultation process. This collaboration is crucial for seizing opportunities to make Australia a global leader in cyber security. The rising volume and velocity of attacks reinforce the critical work of our members, who are the practitioners on the front line of Australia's cyber defence.

We'd like to extend our thanks to the Department of Home Affairs and the Cyber Security Minister's office for their active participation. The team's willingness to meet with AISA representatives to provide context on the consultation paper was greatly appreciated. We encourage this strong spirit of collaboration to continue as the cyber security strategy moves toward implementation.

[redacted]
[redacted] **– AISA Board of Directors**

Developing our vision for Horizon 2

Outlook for Horizon 2

1. 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?

Trend 1: Declining Cyber Security Investment

Declining cyber security spending due to budget cuts and job losses as organisations look to optimise their workforces through AI, and general poor market conditions, could jeopardise the 2023–2030 Australian Cyber Security Strategy's goal of making Australia a global cyber leader by 2030. Reduced funding might stall key Horizon 1 initiatives like Cyber Wardens and SME resilience programs, limiting their rollout in Horizon 2 (2026–2028). The Australian Information Security Association (AISA) recommends locking in sustained investment, teaming up with industry for cost-effective training, and boosting transparency with public metrics to track progress, ensuring resilience against growing cyber risks.

Trend 2: Challenges for New Graduates and Career Changers Entering the Cyber Security Workforce

New graduates and career changers in Australia pursuing cyber security as their chosen profession are facing increasing difficulty securing roles, risking disillusionment and a shift toward non-cyber tech careers, which could undermine the 2023–2030 Australian Cyber Security Strategy's workforce development goals. Despite initiatives like the APS Workforce Plan 2025–30, the global cyber skills shortage of 4 million professionals, coupled with intense competition and limited entry-level roles, may deter both groups, exacerbating Australia's talent gap. With rising cyber threats, the Australian Information Security Association (AISA) advises strengthening partnerships with universities, vocational training, and industry to create structured pathways, such as internships and mentorships, with clear metrics to track placement rates, ensuring the Strategy's empowered workforce shield supports Horizon 2 (2026–2028) objectives for a resilient cyber ecosystem.

Trend 3: Increase in Geopolitical Tensions and Sovereign Capability Challenges

Escalating global conflicts (e.g., US-China rivalry, Russia-Ukraine war, Gaza war) will heighten state-sponsored cyber threats to Australia, including espionage and interference, straining sovereign capabilities like domestic tech production, supply chain resilience, and regional alliances amid uncertainty and export controls.

Trend 4: Acceleration of Government Services Online

The shift of more government services to digital platforms, aiming for full access by 2025 via myGov and Digital ID Bill 2024, will amplify challenges in digital identities, user confidence, and scam protection, with rising impersonation scams (e.g., myGov phishing) and social media fraud eroding trust amid increased online interactions.

Trend 5: Surge in AI-Driven Cyber Threats and Defences

Generative AI will drive sophisticated cyber attacks like phishing, deepfakes, and automated ransomware, while also enhancing threat detection and security operations automation.

Trend 6: Evolving Identity and Access Management (IAM) with AI Agents

The rise of AI agents and digital identities will transform IAM, with AI-driven authentication (e.g., behavioural biometrics) improving security but also introducing risks like AI-powered identity spoofing and credential theft, especially in cloud and remote work environments. This demands adaptive IAM frameworks to secure digital IDs and manage access at scale.

Trend 7: Explosion of Non-Human Identities

Machine identities (e.g., APIs, bots, IoT devices, AI agents) already outnumber humans 20-50:1 and will proliferate with edge computing. Often unmanaged, they create vast attack surfaces, demanding automated governance, certificate management, and continuous validation to prevent breaches.

Trend 8: Quantum Computing Threats and Post-Quantum Cryptography

Quantum computing risks breaking current encryption through “harvest now, decrypt later” attacks by 2030, while Australia’s quantum investments grow. This necessitates urgent adoption of quantum-resistant algorithms to safeguard national security.

Trend 9: Escalation of Ransomware and Supply Chain Attacks

Ransomware and supply chain attacks, amplified by AI and open-source vulnerabilities, will persist, targeting SMBs and critical infrastructure, worsened by decentralised cybercrime networks, requiring stronger ecosystem protections.

Trend 10: Expansion of IoT and Connected Devices

IoT devices, rising to 32 per household by 2027, will widen attack surfaces in operational tech and consumer energy resources, creating new risks and regulatory challenges for secure-by-design standards.

Collaborating across all levels of Australian Government

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

AISA supports collaboration between the federal government and the states and territories. The aim should be to avoid any potential duplication or competition between different governments to ensure the best collective outcome for Australia.

The NSW Digital Skills Compact has been a productive and collaborative mechanism enabling clear discussions between supply and demand owners for cyber skills.

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

3. Does the high-level Model resonate and do you have any suggestions for its refinement?

The high level model provides a useful starting point for developing a measurable and testable theory of change for the cyber security strategy. We look forward to further improvements and iterations.

4. Can you suggest any existing or new ways to collect data and feedback to monitor these outcomes?

AISA recognises the challenges around collecting accurate data for many outcomes. While there may be a limited role for mandatory reporting (eg the recent legislation on reporting ransomware payments), we encourage making use of existing datasets collected across government; noting this may require some innovative approaches in correlating between different datasets.

Shield – level focus for Horizon 2

Shield 1: Strong businesses and citizens

5. What could government to do better target and consolidate its cyber awareness message?

The Australian Government's efforts under the Strategy, including the Act Now Stay Secure campaign, targeted grants for vulnerable communities, and programs like Cyber Health Checks and Cyber Wardens, are impressive steps toward boosting national cyber awareness, backed by significant funding (over $60 million for small businesses) and inclusive outreach to diverse groups. These initiatives have set a solid foundation for strengthening resilience against growing threats like ransomware and scams. However, without clear, publicly available data on campaign costs, participation numbers, engagement levels, and tangible outcomes, such as fewer reported incidents or better cyber hygiene practices, it is difficult to pinpoint exactly how to sharpen targeting and streamline messaging. As a critical first step, the Government could focus on greater transparency by regularly sharing detailed performance metrics and evaluations, allowing for evidence-based tweaks to tailor messages more effectively, optimise resources, and maximise impact across sectors.

To support the Strategy, particularly in addressing the challenge of limited transparency and measurable outcomes in awareness campaigns like Act Now Stay Secure, Cyber Health Checks, Cyber Wardens, and community grants, the Australian Information Security Association (AISA) can offer collaborative expertise. With a network of over 15,000 cyber security professionals, AISA can work with the Australian Cyber Security Centre (ACSC) to refine and deliver targeted educational resources, such as practical guides and workshops, tailored for SMEs and diverse communities during initiatives like Cyber Security Awareness Month. AISA can also contribute to developing consistent metrics frameworks in partnership with the Executive Cyber Council, helping to track participation and impact, addressing the current gap in data, such as user numbers for the Small Business Cyber Resilience Service or the effectiveness of $9.6 million in grants. By facilitating knowledge-sharing through events and platforms, AISA can support the dissemination of tools like Exercise in a Box and sector-specific playbooks, enhancing campaign accessibility and effectiveness while aligning with the Strategy’s goal of a cyber-resilient Australia.

6. **What programs or pilots have been successful in this context? What additional supports could be developed or scaled-up to address these issues in partnership with both education stakeholders and those with technical cyber security expertise?**

The personal cyber health check program was supported by the NSW Department of Enterprise, Investment and Trade and was conducted by GuardWare, an Australian Cyber Security company.

The program was designed to protect small businesses from some of the growing number of cyber threats that are active on-line. It was a highly successful program that provided free risk assessment, conducted by cyber assessment task force (cyber security students) who then developed and presented a custom risk mitigation plan for the organisation based on the identified risks, along with recommendations.

The program gave students opportunities to gain work experience and educated small businesses. This program could be scaled up with the support of Government, Education Providers and AISA to deliver this service nationally.

7. **How can Government encourage SMBs and NFPs to uptake existing cyber resources (i.e. Small Business Cyber Resilience Service, Cyber Wardens, ACNC guidance etc.)?**

Whilst Australian government cyber security initiatives have been encouraging, greater uptake of existing cyber resources by SMBs and NFPs could be enhanced by simplifying access and consolidating all available resources into one location via a centralised hub. Currently, resources like the Small Business Cyber Resilience Service and Cyber Wardens program are scattered across different government websites, making it difficult for businesses to find comprehensive support.

We recommend the following;

- The development sector-specific landing pages and guidance that present resources to different industries and organisation types. NFPs, for example, would benefit from seeing ACNC governance guidance alongside other relevant resources in their specific context and often have limited IT resources and volunteer-heavy structures that require different approaches than traditional businesses.

- Partnering with industry associations and peak bodies to promote resources through existing networks. Professional associations, chambers of commerce, and NFP umbrella organisations already have established relationships and trust with their members.
- Work through local business networks such as regional business enterprise centres, local councils, and small business development organisations that have regular contact with target audiences.
- A shift in messaging to more outcome focused that emphasises business continuity and reputation protection rather than technical security features. Focus on "keeping your business running" rather than "preventing cyber attacks." It is recommended that this include relatable success stories and case studies from similar organisations that have successfully implemented resources, demonstrating practical value and achievable outcomes.

8. 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?

Many SMBs and NFPs rely on external Managed Service Providers to provision and manage their technology systems. There are no mandatory quality or security standards in place for these providers, and many SMBs and NFPs are not aware that secure operations are not a default. In some cases these organisations are unaware they are at risk, in other cases MSPs recommend security controls, but small organisations opt not to implement them due to cost. The government should consider MSPs as a vector to improve cyber security and resilience among SMBs and NFPs.

9. **What existing or developing cyber security standards, could be used to assist cyber uplift for SMBs and NFP's?**

ACSC Essential Eight is a recognised baseline framework The Essential Eight maturity levels allow organisations to assess the appropriateness of their cyber security measures against common threats. This is particularly suitable for SMBs and NFPs as it provides a practical, government-endorsed baseline, however additional support for NFPs and SME's is required in implementing the Essential Eight given the limited staff resources these types of organisations have.

The combination of the Essential Eight framework with support from programs like Cyber Wardens and potential grant funding through the Small Business Cyber Resilience Service creates a comprehensive ecosystem for cyber uplift that's both accessible and locally relevant.

10. **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?**

Not-for-profit (NFP) entities in Australia face distinct cyber security hurdles under the 2023-2030 Australian Cyber Security Strategy, primarily stemming from resource constraints and operational models that differ from profit-driven businesses. Key challenges include severely limited budgets and expertise, with 88% of NFPs allocating no funds to cyber security and 80% providing no recent training to staff or volunteers, leading to low digital competency (57% rate as "average" and 31% needing improvement) and uncertainty in data privacy compliance (41% unsure how they handle it, only one-third compliant). This contrasts with broader businesses, which often have dedicated IT teams, profit incentives to invest in defences, and higher rates of supplier due diligence (though still low at 29%), enabling better preparedness despite similar threats like phishing and ransomware. NFPs' reliance on part-time staff, volunteers, and personal devices exacerbates vulnerabilities, making centralised security harder, while handling sensitive donor or client data for

88% of NFPs allocating no funds to cyber security and 80% providing no recent training to staff or volunteers

NFPs are the second-most targeted sector globally for nation-state attacks (31%),

vulnerable populations heightens breach impacts—one in five fears total devastation from an attack, compared to businesses' greater resilience through diversified resources. Additionally, NFPs are the second-most targeted sector globally for nation-state attacks (31%), yet de-prioritise security for mission-focused activities, facing barriers like funding shortages (61%) and skilled resource access (37%), unlike businesses that can leverage economies of scale. Insider threats, third-party vendor risks, and natural disaster disruptions further compound issues, with only 49% having information security policies due to uncertainty or perceived irrelevance.

High-Impact Government Interventions for the NFP Sector

Aligned with the Strategy's "Strong Businesses and Citizens" shield, the most impactful interventions would extend small business supports to NFPs, such as targeted grants (e.g., expanding the $9.6 million community awareness program to fund NFP-specific cyber tools and training, addressing the 87% without documented improvement plans). Providing free cyber health checks and resilience services, similar to those for 2.5 million small businesses, could uplift NFPs' capabilities, given their 1-in-8 breach rate and resource strains amid rising service demands. Tailored education via partnerships (e.g., with the ACNC for compliance under the Privacy Act) and a 10-year digital roadmap through an expert group would build skills, while integrating NFPs into threat-sharing networks and exercises could enhance resilience, mirroring calls for government-funded "mission-critical" solutions to protect vulnerable data and prevent reputational damage. These measures, building on Strategy consultations with NFPs, would maximize impact by equating support to that for businesses, fostering sector-wide uplift.

By participating in consultations and the Executive Cyber Council, AISA can help bridge the gap between government initiatives and NFP needs, fostering public-private collaborations to uplift sector-wide cyber maturity and prevent breaches that could devastate mission-critical services.

https://www.uwa.edu.au/schools/-/media/Centre-for-Public-Value/Resources/230906-State-of-the-Sector-Report.pdf
https://www.communitydirectors.com.au/articles/charities-in-fear-of-cybercrime-report

https://www.communitydirectors.com.au/articles/nfps-struggle-to-manage-cyber-security-risk-report
https://www.aicd.com.au/risk-management/framework/cyber-security/cybersecurity-remains-top-concern-for-australian-businesses.html
https://probonoaustralia.com.au/news/2023/01/charities-more-vulnerable-to-cyber-attacks/
https://www.infoxchange.org/au/news/2023/11/not-profit-sector-response-australian-government-cyber-security-announcement

11. Do you consider cyber insurance products to be affordable and accessible, particularly for small entities? If not, what factors are holding back uptake of cyber insurance?

Insurance has played a significant role in risk management and mitigation in other sectors, e.g. employer liability, but currently does not seem to operating effectively for cyber security in Australia. Many businesses report that premiums are high and the scope is often limited. The underlying causes are not clear, but we recommend further engagement with the insurers and underwriters, in particular on the quality of information available to them to effectively price their policies and adjust pricing based on client profile and behaviour.

12. How well do you consider you understand the threat of ransomware, particularly for individuals and small entities? How is this threat evolving or changing?

Ransomware is a threat that all entities are aware of, and continues to be one of the top threats to small businesses and organisations.

13. How could the government further support businesses and individuals to protect themselves from ransomware attacks?

Effective support to protect against ransomware requires a full spectrum of measures, including education, threat-blocking and targeted disruptions of criminal infrastructure and activity.

16. Which regulations do you consider most important in reducing overall cyber risk in Australia?

Australia has implemented a range of regulations, recognising that different approaches and nuance are required in different circumstances. Particular examples that we commend are mandatory labelling of smart devices so that consumers can be suitably informed, and the overall SOCI approach of considering security holistically and encouraging a risk-based approach.

Personal liability for directors under the Corporations Act 2001 has elevated cyber security to a boardroom issue where it previously may not have been. While this doesn't correlate directly to reduced risk, AISA members have noted a shift in focus following these changes.

17. Have regulatory/compliance requirements negatively impacted the cyber maturity of your organisation? How are you currently managing these issues?

Although AISA has not been significantly impacted, we are aware of the challenges faced by other organisations. For example, the requirement for all DISP entities to meet Essential 8 Maturity Level 2 can be very onerous, as demonstrated by the fact that many Government departments cannot meet this despite having significant teams and resources to devote to IT security. We encourage a proportionate, risk-based approach when specifying compliance requirements.

Shield 2: Safe technology

19. 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?

Educating the public to protect themselves from cyber threats is a core part of AISA's mission. We would be happy to engage with the Government to identify the messages and target audiences where we can help with this mission.

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

Although generic advice is broadly available and understood, it would be helpful to have advice on practical application. This could include examples of acceptable and unacceptable risks, and a way for organisations to access some form of FOCI assessment on vendors for sensitive applications.

21. 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?

Government can help in education and guidance around the minimisation of data collection, and methods for sharing that minimise security risks while maximising benefits. This could also include supporting research in to developing fields such as homomorphic encryption, privacy-preserving techniques and data de-identification.

We also note the role that digital identity can play in reducing the collection and sharing of personal information. The Digital ID Act passed last year is a valuable first step, but closer co-ordination is required between the plans for the Australian Government Digital Identity System and private sector systems such as ConnectID that are gaining momentum.

22. 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?

As noted above, Government can help in education and guidance around methods for sharing that minimise security risks while maximising benefits. This could also include supporting research in to developing fields such as homomorphic encryption, privacy-preserving techniques and data de-identification.

23. What guidance can government provide to support the safe and responsible uptake of critical and emerging technologies?

Critical and emerging technologies can introduce new risks and opportunities that may not be immediately obvious to many potential users. In order to provide effective advice, the government should draw upon experts with detailed understanding of the technology, combined with cyber risk professionals and effective communicators, and use this to develop understandable, pragmatic and actionable advice.

Shield 3: World-class threat sharing and blocking

24. 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?

A proactive security posture would require adoption of secure-by-design and secure-by-default approaches across industry. The role of government can be to educate and provide guidance on how to achieve this, and identify potential interventions to influence the behaviour of those who are best placed to make such changes, for example technology providers.

25. Does the government need to scope and define what Australia's proactive cyber security posture should look like for industry?

Yes, as noted above a key role Government can play is in education and guidance.

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

The government should identify the infrastructure operators in the best position to block threats, provide legal clarity for them to do so, and support with appropriate threat intelligence so that they can do so effectively.

28. 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?

The CI-ISAC has had encouraging results. We encourage the Government to learn from what has worked well and how this could be translated to other sectors. We also encourage clear definition of what actions can be taken by organisations based on threat sharing data - for example the role of active cyber defence.

29. How can we better align and operationalise intelligence sharing for cyber security and scams prevention?

Intelligence sharing appears to work well when initiated and run by industry (eg the ISAC model). Government should be an active contributor, by finding ways to rapidly declassify and share machine readable threat intelligence to such threat sharing hubs.

30. 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?

The appointment of the National Cyber Security Co-ordinator has helped to move forward the discourse on this topic. However, we believe there is still room for improvement and encourage running exercises with a full range of stakeholders. AISA would be happy to participate in, and potentially help to facilitate such exercises.

31. How could government better incentivise businesses to adopt vulnerability disclosure policies?

The appropriateness of a formal vulnerability disclosure policy will vary by organisation. However, the Government can help by providing clearer guidance for relevant sectors as to how such a policy could fit in as part of an overall risk management and best practice approach.

32. Does Australia need a vulnerability disclosure program to provide security researchers with a mechanism for safely reporting vulnerabilities?

As a minimum, we recommend providing legal clarity on what is acceptable research activity and how the results should be handled. We recommend that the Government consults with all sectors of industry before considering introducing some sort of national level solution – there should be clear evidence of a failure of other mechanisms to justify such an approach and ensure it is fine tuned to address such gaps.

Shield 4: Protected critical infrastructure

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

Australia has demonstrated global leadership with the SOCI Act covering a broad range of critical infrastructure sectors, taking an all-hazards approach and driving a risk management mindset. As the Government expands and refines the regulatory regime, we encourage close collaboration with the relevant industry and technology experts. For example, recent initiatives to mandate Essential 8 maturity reporting may be well-intentioned but drive undesirable behaviour. Although the Essential 8 is good starting point for internet-facing office IT networks, it is not suitable for many critical infrastructure systems. In particular, for operational technology systems other standards such as by NIST CSF are much more relevant.

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

Under the existing framework, a broad range of risks are considered through an all-hazards approach. We concur that the proposed model of sector-specific measures presents a significant opportunity. Given that certain risks are unique to individual sectors, it is not efficient to impose this burden on all entities. We are supportive of this approach and welcome the ability to develop tailored requirements that create appropriately scaled obligations and regulations based on risk.

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

Overall, both organisations and industry are experiencing a significant regulatory burden, not only within cyber security but across various domains. While the need for regulation is acknowledged, there is a distinct opportunity to build on the work from Horizon One to better harmonize regulations and obligations.

The focus on targeted regulation for Critical Infrastructure, alongside a general uplift in the business population's cyber security, is broadly supported. However, we caution against overly prescriptive legislative requirements, as the pace of evolving security risks can outstrip regulatory updates. We believe that aligning with universal frameworks is a more effective mechanism for ensuring compliance.

36. 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?

The government has several opportunities to partner with critical infrastructure owners and operators to improve their cybersecurity practices.

One key area is providing practical tools and guidance. This could include expanding the targeted playbooks and materials to help organisations improve their controls against specific frameworks. Additionally, sharing lessons from exercises or real-world incidents in an easy-to-digest format would enable rapid mitigation of evolving threats, like the recent surge in social engineering attacks. Sharing incident response learnings would also ensure rapid adoption of new best practices.

There is also strong interest in financial incentives, such as tax breaks or other mechanisms, to reward entities that significantly invest in their cybersecurity capabilities. Implementing mature controls is often a costly exercise that competes with other business priorities, and incentives would encourage stronger security postures.

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

There is an opportunity for the Government to map their specific security requirements and the regulatory obligations against the common frameworks and best-practices applicable. This would not only streamline compliance for businesses but also allow them to benchmark their security posture against government-only requirements and identify areas for greater focus.

Furthermore, providing insights and recommendations on practical implementation—including the ideal order of operations and lessons learned from past projects—would significantly enhance industry engagement and the overall effectiveness of security uplift initiatives

38. How are Australian Government security requirements or frameworks being considered or adopted among private sector partners, including in critical infrastructure?

We're observing a trend where organisations are prioritizing industry best practices and frameworks, then adding specific government requirements. As we've noted, aligning government controls with these common frameworks or providing a mapping tool would enable organisations to more easily conduct gap analyses.

Shield 5: Sovereign Capabilities

39. 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?

A skilled, diverse and adaptable cyber security workforce is a matter of national security, and, as such, should continue to be supported by the government. The use of mechanisms like Jobs and Skills Councils and the NSW Digital Skills Compact to better align supply and demand mechanisms should continue.

Initiatives like the Institute of Applied Technology - Digital, that represent public-private partnership to make job-ready cyber skills accessible support our workforce. Further effort should be undertaken to market these offerings to employers.

One major challenge that remains is the lack of junior roles available in cyber security disciplines. Many graduates report challenges in finding a role in our industry. With the growing impacts of AI tools on junior roles, the government should explore the impact on junior cyber security roles and incentives for employers to engage in the training system.

One major challenge that remains is the lack of junior roles available in cyber security disciplines.

Many graduates report challenges in finding a role in our industry.

Clear pathways and expectations of professionals in our critical sector support workforce development. While professionalisation has not yet been piloted and may not be appropriate for all areas of our industry, it may benefit the industry through clear definition of pathways and requisite skills.

40. What have been the most successful initiatives and programs that support mid-career transitions into the cyber workforce and greater diversity in technology or STEM-fields more broadly?

The cyber security workforce greatly benefits from mid-career entrants to our industry and the rich skillsets that these career changers bring.

Many mid-career entrants to our industry come from adjacent roles, like network engineering or IT support. By making short courses or stackable credentials accessible

to these workers, they can more easily transition into cyber security roles, or apply cyber concepts in their existing roles.

Mid-career entrants are far more likely to have existing financial commitments. Earn While You Learn pathways are critical to supporting this cohort.

Supporting diversity in cyber security is a priority for AISA. While our sector has strong representation of CALD groups, we have room to improve particularly in the representation of women and first nations Australians in our workforce. Given the increasing nature of cyber threats, and the often deeply personal impacts on victims of cyber-crime, it is critical that our sector is representative of the population it serves.

To continue to diversify our workforce, AISA has undertaken several initiatives:

- **Pride in Security is a special interest group among our members that promotes inclusion and allyship of LGBITQA+ individuals in our industry**
- **The AISA scholarship fund supports diverse entrants into our workforce with financial and professional support through their tertiary education**
- **Extensive support for Women in Security initiatives including events and awards promoting the inclusion and celebration of the achievements of women in our workforce.**

41. What are some of the industries with highly transferrable skill sets that could be leveraged to surge into the cyber workforce? Is there any existing research/data that could support these efforts?

By taking a skills first approach to the workforce, rather than focusing on specific qualifications or certifications, we can more readily identify those with transferable skills.

Skills frameworks like SFIA or commercially available tools like Rejig can be quickly applied to map these skill sets reliably.

The cyber workforce can be surged in two ways - by adding more skilled workers to cyber specific job roles, or by moving security tasks into adjacent job roles, like software engineering. The later approach is also known as 'shifting left', whereby cyber security tasks are moved into roles earlier in the production of technology products. While this is not applicable for every cyber security task (for example ongoing monitoring in a SOC), it can be used to upskill other workers, improve resilience of new technology products, and reduce the number of headcount dedicated only to cyber security in a given organisation. This can be appealing when budgets and headcounts are tight.

42. 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?

AISA commends the thorough consultation undertaken in the last 3 years regarding the Cyber Strategy. This type of tri-partite consultation, paired with ongoing mechanisms like the Executive Cyber Council, has allowed a closer alignment on priorities. AISA would like to see the ongoing components like the ECC and CIRB continued and expanded. We would like to offer our expertise and ability to represent cyber security professionals in these forums.

Further to alignment on priorities, AISA believe a key factor to encouraging innovation in cyber security is supporting Australian cyber security startups. It remains extremely difficult for cyber security startups to scale in Australia without moving offshore for access to capital and customers. Government and industry can support ongoing innovation and healthy competition in the Australian cyber security ecosystem by adopting local solutions.

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

Sovereign capability is an important subject, but multi-faceted and often misunderstood. We recommend creation of an assessment framework that identifies what aspects of a technology need to be sovereign and why, and using this to prioritise appropriate government investment.

Shield 6: Strong region and global leadership

46. 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?

AISA applauds the governments work in recent years to use attributions, advisories and sanctions. These provide valuable public signalling and potential deterrence. We also support the use of targeted interventions to attack the infrastructure and capabilities used by threat actors.

47. Are there additional ways the Australian Government could engage with Southeast Asia or the Pacific to ensure a holistic approach to regional cyber security?

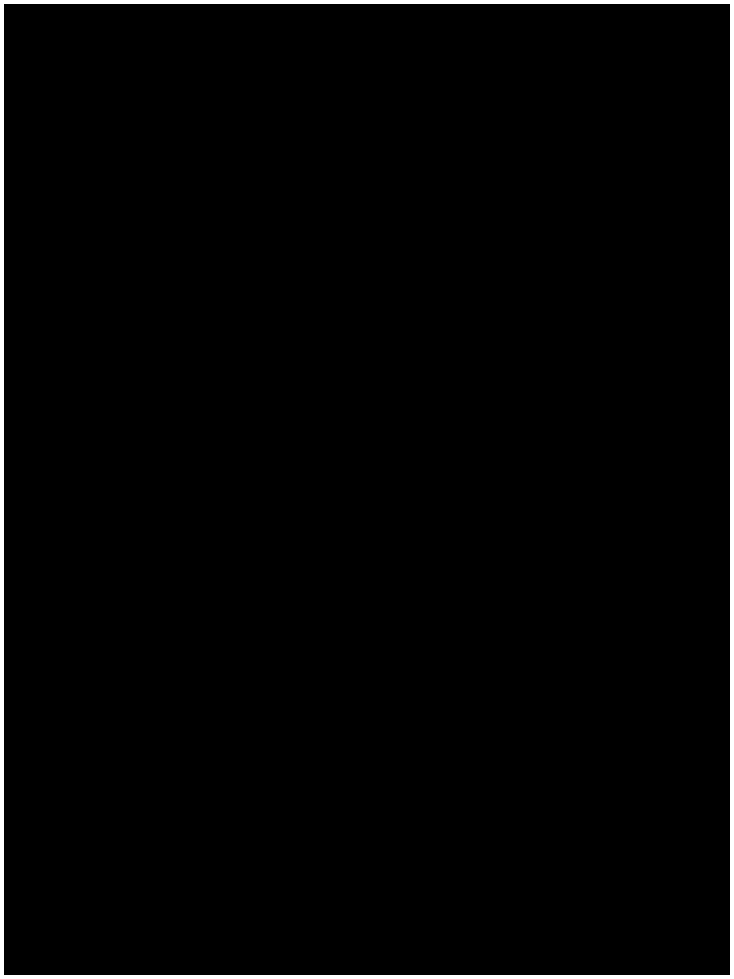
The Government should work with other regional governments to share best practice and to help these organisations to build cyber resilience into their economies.

48. Is there additional value that Cyber RAPID can provide in the region beyond its current design and scope?

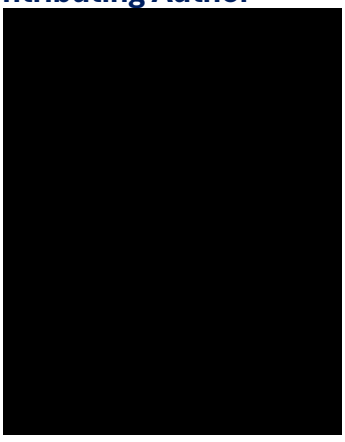
We propose that Cyber RAPID should help regional governments to build lasting capability that reduce the likelihood and impact of future incidents.

Authors

Lead Authors



Contributing Author



AISA Australian Information Security Association

Australian Information Security Association (AISA)

ABN 181 719 35 959

[redacted]

[redacted] | www.aisa.org.au