SANS

Horizon Two Consultation Discussion Paper

SANS Training Australia

[redacted]

SANS | GIAC CERTIFICATIONS

Introduction

SANS Institute is pleased to contribute to the Horizon 2 consultation process for Australia's Cyber Security Strategy. Australia's Horizon 2 consultation paper sets out targeted actions across the "Six Shields" (Prepare, Prevent, Protect, Pursue, Recover, and Engage) and invites submissions to shape concrete programmes before the 2030 Strategy midpoint. SANS strongly supports Horizon 2's emphasis on uplift at scale and offers evidence-based recommendations with a focus on Workforce uplift.

SANS has trained tens of thousands of cyber security professionals worldwide, partnered with governments and enterprises to uplift cyber capability, and conducted workforce research that directly informs policy development. We bring practitioner-led expertise, evidence from academy (rapid re-skilling) programmes, and global insight into what drives effective workforce development. We submit that while workforce initiatives make up a smaller portion of the consultation paper by length, they are in fact the biggest enabler of Horizon 2 success. Regulatory reforms, technology deployments, and awareness programmes cannot deliver outcomes without a skilled workforce to implement and sustain them. Workforce investment is the multiplier that makes every Shield operational. Workforce is not one Shield among six, it is the cross-cutting enabler of every Shield.

This response to Horizon 2's consultation paper will support the existing emphasis on uplift at scale and offers evidence-based recommendations for workforce uplift, grounded in global research and existing case studies from across the world. Lessons identified from other countries, enterprises, and cyber industries, as well as considerations for alternate professions/industries, have been included in this response. Analysis of previous successes has been used to provide recommendations for programmes and priority initiatives for Horizon Two, to achieve the Strategy's ambition of making Australia the most cyber secure nation by 2030.

Key Recommendations

The recommendations included in this response to the Horizon Two consultation paper are focused on Workforce as a critical enabler across all Six Shields. SANS recommends that Horizon Two focus on the following to uplift the cyber workforce: shift from headcount to skills; standardise role definitions; invest in training and certification, including prioritisation of critical skills roles; and scale onramps that can rapidly place diverse Australians into critical cyber roles.

1. **Skills over seat counts:** Horizon 2's focus on practical uplift aligns with what we see globally: organisations struggle more with having the right skills than with pure vacancy numbers. In 2025 data, 52% cite "not having the right staff" vs 48% "not enough staff" (SANS & GIAC, 2025), Australia needs a decisive shift to skills-based workforce planning, aligning with a competency based professionalisation framework.

2. **Standards, assurance and regulation drive behaviour:** New and evolving directives internationally (e.g., Network and Information Security Directive 2 (NIS2), Digital Operational Resilience Act (DORA), SEC/Cybersecurity Maturity Model Certification (CMMC)) are already changing hiring and training; 40% of organisations report privacy and compliance risks affect hiring, and 65% require formal skills validation for internal or external assurance. Designing Horizon 2 programmes with explicit competency evidence (e.g. qualifications, certifications, credentials etc) will accelerate adoption.

3. **National cyber competency framework (practical, role based):** Prioritise the delivery of the national cyber competency/professionalisation framework. The professionalisation framework should leverage existing globally recognised programmes, which focus on critical skills, and require validation of competency.

4. **Outcome based funding for workforce programmes:** Tie grants to measurable results: certifications/qualifications earned; time to placement; and retention for12 months or longer. There are multiple international examples of competency-led, rapid re-skilling programmes (often referred to as Cyber Academies), which have a proven record for extremely high (>80%) employment rates on program completion, with associated validation of competencies (i.e. certifications). These programs have been very successful, including for career changers, women and other underrepresented groups.

5. **Certification anchored supply chain uplift:** For small/medium enterprises supplying critical sectors, co-fund short, role-based skilling with third-party validation to meet insurer, auditor, and customer requirements mirroring the 65% client driven validation trend.

6. **Targeted on ramps for underrepresented Australians:**
   Scale scholarship-based reskilling for women, veterans, Indigenous Australians, regional/rural talent, participants from socio-economically disadvantaged backgrounds

and career changers, modelled on existing national and global programmes that deliver high pass and placement rates at speed.

7. **Sector academies for critical roles:**
   Stand up national academies for critical roles including Industrial Control Systems (ICS)/OT, Digital Forensics, Incident Response and Digital Evidence, Artificial Intelligence Security and Security Operations Centre (SOC) analyst.

8. **Employer enablement:**
   Provide toolkits for HR-Cyber collaboration (structured job families, realistic requisitions, mentorship blueprints, skills assessment rubrics). Studies show HR and cyber leaders often misperceive who has hiring authority and which qualifications matter; bridging that gap speeds hiring and improves fit.

Response to Horizon 2 Annex A - Consultation Questions

The focus of SANS Institute's responses to this section remains on the cyber security workforce. Please note, some of the questions have been grouped together to support a consolidated response.

Outlook for Horizon 2

Question 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?

Australia's cyber threat landscape is being reshaped by advances in Artificial Intelligence (AI), operational technology (OT)/industrial control systems (ICS), and quantum computing. Artificial Intelligence (AI) security is emerging as the fastest-growing gap, with a projected shortage of ~34,000 Artificial Intelligence (AI) security professionals by 2030[1].

OT/ICS engineering roles are equally critical, underpinning critical infrastructure resilience. These roles already take 69 days (or 25% longer) to fill on average compared with 55 days for generalist positions (SANS & GIAC, 2025)[2]and are projected to fall short by 26,000 professionals by 2030. Horizon 2 must prioritise domestic pipelines for Artificial Intelligence (AI) assurance and OT/ICS engineering, to secure critical services and maintain competitiveness. Workforce implications from the development and implementation at scale of quantum computing are still emerging, and robust quantitative data on shortages are not yet available.

Global shortages in critical roles such as OT/ICS and AI security are the binding constraint for Australia's resilience. Addressing this through National Academies or other rapid re-skilling initiatives, scholarships, apprenticeships, and certification-driven programmes will unlock the capacity required to achieve the Strategy's ambition of making Australia the most cyber secure nation by 2030.

[1] *This figure is a conservative modelling assumption extrapolated from global trends rather than a published national forecast (ISC², 2023).*

[2] *This estimate is based on extrapolation of current global workforce data and scaled for Australia [WEF, 2024].*

Collaborating across all levels of Australian Government

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

Several state-level programmes, including STEM-in-schools and vocational training via TAFE, have shown success in attracting non-traditional entrants. Veterans' transition schemes also provide strong pipelines. These should be scaled nationally into a unified academy framework. International models demonstrate demand: the Rogers Cybersecure Catalyst (Rogers Cybersecure Catalyst, 2023) in Canada trained over 700 career-changers with 11 applicants for every available place, highlighting untapped talent pools.

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

The Government's proposed Policy Evaluation Model is sound, but metrics must focus on outcomes. KPIs should include job placement within 12 months, skills validation (certifications), retention at 12-24 months, diversity participation, and role-specific capacity in OT/ICS and AI. Evidence shows 65% of organisations globally now require formal skills validation for compliance or client assurance (SANS & GIAC, 2025). Publishing quarterly dashboards would replicate Horizon 1's transparency and maintain stakeholder confidence.

Shield 1: Strong businesses and citizens

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

Awareness campaigns must be consistent nationwide and tailored to vulnerable cohorts such as seniors, First Nations, and CALD communities. School programmes should incorporate hands-on cyber activities and gamified labs, as these approaches improve engagement. International models, such as Women in Cybersecurity (WiCyS) (WiCyS, 2025) and Catalyst (Rogers Cybersecure Catalyst, 2023), demonstrate that early exposure increases diversity and strengthens long-term pipelines.

Question 6. What programmes 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?

There are numerous examples of best-practice cyber awareness campaigns being successfully deployed to help mitigate cyber risk. The United Arab Emirates launched a 'Cyber Pulse Initiative' in 2021, that seeks to engage the broader community in matters of cyber security (UAE, CSC, 2024). It launched a significant public awareness campaign, including training courses, workshops and lectures about cyber security, to inform the public on how they can protect themselves. The first phase targeted women and children, and the second targeted students (UAE, 2024). These programs were executed by public-private partnerships, and have shown very strong results, which is reflected in the UAE's position on the Global Cyber Security Index in 2024 (World Economic Forum, 2025).

Another useful but different international example is Saudi Arabia's whole-of-society cyber awareness model, where campaigns are positioned as a public good and made widely available to all citizens (Saudi National Cybersecurity Authority, 2025). The Saudi National Cybersecurity Authority has run campaigns using national media and celebrity ambassadors to normalise everyday cyber hygiene. This demonstrates the impact of combining consistent nationwide messaging with broad accessibility and popular engagement techniques. Australia could consider similar approaches, expanding awareness beyond technical language into mainstream campaigns that resonate with all demographics, potentially using prominent national figures to reinforce simple, repeatable actions.

Question 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?

NFPs face rising costs and limited capacity. The challenges they face are similar to those experienced by small and medium businesses (SMBs). The Australian Signals Directorate (ASD) Annual Cyber Threat Report indicates cybercrime costs rose 8% for SMBs from 2022-23 to 2023-24, an average cost to Small Business of $49,600 (ASD, 2024). Horizon 2 should deliver simplified baseline standards, backed by micro-grants for training and certification. Standards must include OT and AI readiness, reflecting SMB uptake of IoT and automation. Subsidised vouchers for competency/certification linked training would reduce financial barriers.

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

Ransomware remains a major threat. The government should expand awareness through free playbooks and tabletop exercises, especially targeting SMBs. International collaborations such as the Counter Ransomware Initiative should continue. OT-specific preparedness programmes are needed for utilities, healthcare, and transport, where downtime risks are greatest.

Shield 2: Safe technology

Australia should set minimum security baselines for edge and consumer devices to provide consistent protection across households and businesses. However, achieving compliance will require a skilled workforce of product assessors, auditors, and regulators capable of applying these standards in practice. To support this, a national AI assurance workforce program should be developed, focused on adversarial testing, bias detection, and safe deployment. Global experience shows that more than 40% of organisations report their hiring is already shaped by regulatory directives such as NIS II and DORA, and 65% require skills validation for compliance or client assurance (SANS & GIAC, 2025). Embedding these requirements into workforce training ensures that emerging Australian standards are enforceable and trusted by industry.

Data security standards should also be expanded to incorporate AI governance and quantum resilience, but this too depends on talent pipelines. A specialist workforce in post-quantum cryptography, AI ethics, and secure algorithm development will be needed to implement these frameworks. National academies or scholarship-to-job programmes could accelerate workforce readiness, ensuring that Australia develops sovereign expertise in these cutting-edge areas rather than relying solely on imported solutions.

Shield 3: World-class threat sharing and blocking

Threat sharing must be scaled into a whole-of-economy capability, moving beyond the current concentration in high-maturity sectors such as finance and telecommunications. To achieve this, Australia will need to train and sustain additional analysts for Information Sharing and Analysis Centres (ISACs) across sectors including healthcare, energy, transport, and education, where cyber maturity remains uneven. International examples, such as the US sector-specific ISACs and the EU's promotion of ISAC models under the NIS II Directive, show that sector-based collaboration provides trusted mechanisms for sharing actionable threat intelligence (NIS-II, 2025).

At the same time, the scope of Active Cyber Defence (ACD) roles must be clarified in Australian regulation. Clear legal boundaries would allow private and public organisations to adopt proactive defensive measures without fear of liability, while deterring escalation into offensive activity. This aligns with international moves to define permissible defensive practices under frameworks like EU NIS II Directive Article 29 - Information Sharing (2022). Equally important is the creation of safe harbour policies for vulnerability disclosure researchers. Currently, researchers face disincentives to report vulnerabilities due to potential legal consequences, leading to missed opportunities for remediation.

Establishing a coordinated vulnerability disclosure regime, supported by liability protections, would encourage responsible disclosure and significantly reduce the exploitation window for attackers.

Finally, the rapid rise of Artificial Intelligence (AI) and generative AI tools creates new avenues for malicious activity, such as automated phishing, deepfakes, or large-scale disinformation campaigns. Training AI specialists specifically to detect, monitor, and mitigate these threats will be critical to maintaining trust in digital ecosystems. Embedding AI-related threat detection skills into national ISACs and government cyber agencies will ensure that Australia remains resilient as adversaries integrate AI into their attack toolkits (SANS & GIAC, 2025).

Shield 4: Protected critical infrastructure

Question 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?

Supporting Information Sharing and Analysis Centres (ISACs) provides a proven pathway for uplifting resilience across critical sectors. ISACs, already well-established in the US and Europe, enable trusted collaboration within sectors to share actionable threat intelligence and best practices (Electricity – Information Sharing and Analysis Centre, 2025). For example, the European Union Agency for Cybersecurity highlights ISACs as vital sectoral collaboration models (ENISA, 2022), while Article 29 of the EU's NIS II Directive (2016) encourages mechanisms for joint situational awareness and information sharing). The US Cybersecurity and Infrastructure Security Agency (CISA) similarly treats ISACs as "vital resources" for protecting critical sectors (CISA, 2015). Rather than creating new structures, Horizon 2 could expand support for existing or emerging ISACs, particularly in low-maturity sectors, providing funding, regulatory support, and technical enablement. This approach would avoid duplication while reinforcing trusted sector-led coordination.

One of the most effective ways to assist critical infrastructure owners and operators to mature their cyber and operational resilience is through national and industry-led cyber exercises that combine both technical and organisational preparedness. Government can play a convening and enabling role by funding and coordinating tabletop exercises, sector-specific scenarios, and live-fire cyber ranges that simulate real-world incidents such as ransomware, ICS/OT disruption, or supply chain compromise. These exercises help operators identify capability gaps, test escalation pathways, and build trusted relationships across industry and government (ENISA, Cross Sector Exercise Requirements, 2022). For example, Singapore's Exercise Cyber Star 2025, coordinated by the Cyber Security Agency (CSA) of Singapore, brought together 11 critical sectors for 11 days of integrated simulations, blending ICS-focused live-range challenges with command-post exercises across healthcare, maritime,

and transport sectors (CSA SG, 2025). Even simple, low-cost tabletop exercises offer significant value by enabling organisations to practice their incident response plans in a safe setting, clarify roles and communication, and detect weaknesses in a low-disruption environment. Australia could adopt a similar model by expanding the National Cyber Exercise Program into an annual calendar of cross-sectoral simulations and cyber ranges, complemented by incentives such as grants, regulatory recognition, or reduced insurance premiums for organisations that participate and demonstrate improvement. By doing so, government not only uplifts baseline resilience but also fosters a culture of continuous learning and preparedness across the most critical parts of the economy.

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

Critical infrastructure must be supported through sector-specific training programmes in OT/ICS, AI-enabled ICS, and Digital Forensics and Incident Response (DFIR). While regulatory obligations under the SOCI Act set the foundation, workforce readiness will ultimately determine whether operators can comply effectively. Evidence shows that specialised roles such as OT/ICS engineers take on average 69 days to fill compared with 55 days for generalist roles, highlighting the acute talent shortage in these areas (SANS & GIAC, 2025).

To address this, Horizon 2 should expand co-funded training programmes, resilience tools, and scholarships targeted at critical infrastructure operators and their supply chains. Government can play an enabling role by subsidising professional certifications, creating portable credentials, and supporting Information Sharing and Analysis Centres (ISACs) to share both threat intelligence and workforce best practice across sectors (ENISA, 2022).

In addition, uplifting resilience requires a focus on embedding cyber training into operational roles. Many engineers, technicians, and operators already working in energy, water, health, and transport sectors could be rapidly upskilled through targeted bridging programmes aligned to frameworks like NICE and ECSF (NICE (NIST), 2020). This approach builds on their existing domain expertise, accelerating the development of cyber-competent practitioners who understand both the technology and the operational environment. Investing in these human capabilities is essential for ensuring that regulatory standards translate into practical resilience on the ground.

Independent audits under the SOCI Act should also be increased to ensure that critical infrastructure entities are not only meeting compliance requirements on paper but are actively implementing and sustaining effective security controls. Regular third-party assessments provide an objective check on cyber resilience, help identify systemic vulnerabilities across sectors, and build confidence for government, regulators, and the community. Embedding workforce considerations into these audits such as verifying staff competencies, training records, and incident response readiness would also ensure that compliance is tied to the human capability needed to defend critical systems.

Shield 5: Sovereign capabilities

Question 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?

Evidence from the World Economic Forum (2024) highlights a global shortage of 4 million cyber security professionals, projected to rise to 85 million by 2030. Australia's domestic workforce challenges mirror this trend, with rising recruitment costs and talent shortages impacting national productivity. To achieve a sustainable, diverse, and future-ready cyber workforce, the Government must act simultaneously as an enabler, convener, and regulator. Australia should build on Horizon 1 initiatives, such as the Growing and Professionalising the Cyber Workforce grant, by scaling funding for professionalisation schemes, embedding standardised frameworks like NICE and ECSF, and strengthening pathways between academia, industry, and government.

As an **enabler**, it can fund targeted programs such as outcome-based grants, sector academies, and professionalisation pilots that accelerate job-ready skills. As a **convener**, it should align employers, educators, and regulators around a National Cyber Competency Framework and provide employer toolkits that harmonise hiring practices with validated skills. As a **regulator**, it must ensure minimum standards and assurance mechanisms are in place, so that certifications and skills recognition have credibility across industry, insurers, and customers. Together, these roles underpin the six proposed actions: shifting focus from headcount to skills, establishing a national framework, professionalising credentials, funding tied to outcomes, creating sector academies, and enabling employers to structure and retain talent.

1. Shift from headcount to skills: Workforce gaps are increasingly about "not the right staff" (52%) versus "not enough staff" (48%) (SANS & GIAC, 2025). Policies should prioritise validated skills over raw numbers.

2. The Cyber Professionalisation Grant should prioritise delivery of a national framework that leverages existing and globally recognized frameworks. SANS recommends the National Cyber Competency Framework aligned to NICE/ECSF but tailored to Australian needs (e.g. OT/ICS, AI security, digital forensics) as 46-52% of global organisations already using these frameworks, as well as close partner nations (SANS & GIAC, 2025).

3. Professionalisation pilots: Fund portable, certification-anchored credentials that allow mid-career entrants and SMEs to meet insurer, regulator, and customer assurance requirements.

4. Outcome-based funding: Tie grants to job placements, certifications achieved, and 12-24 month retention.

5. Sector academies for critical roles: Stand up national competency-based, rapid re-skilling programmes ('Academies') for ICS/OT engineers (69 days to hire), SOC analysts/incident responders (79 days to hire), and AI security specialists (SANS & GIAC, 2025).

6. Employer enablement: Provide toolkits for HR-Cyber collaboration (structured job families, mentorship frameworks, competency rubrics).

Leveraging existing programs globally will provide Australia to quickly uplift its Cyber Workforce. Not only will it reduce the time required to design and implement a professionalisation program, but it will also align Australia's skillsets to a global standard, which reduces barriers across enterprises and governments. Examples of programs run by government organisations are included below. It would be inefficient to attempt to develop world-class sovereign capability in Australia without leveraging existing world-class capabilities and expertise from around the globe.

The U.S. Department of Defence's DoD 8140 directive (2023) mandates workforce role alignment and skills validation. The Department of Defense Directive 8140 requires all military, civilian, and contractor personnel to validate their skills for specific cyber work roles. This validation can be achieved through professional certifications, military schoolhouse training, accredited academic programs in cybersecurity, or relevant work experience. The directive was designed to give the Department of Defense a comprehensive view of its cyber workforce, helping to identify critical skill gaps and prioritize efforts to address them. Ultimately, DoDD 8140 establishes a standardized system to track, manage, and enhance workforce readiness.

An additional international model worth monitoring is the UK's Chartered Status program (the local terminology for license), led by the UK Cyber Security Council (a collaboration with the UK Department for Science, Innovation and Technology – DSIT / UK National Cyber Security Centre - NCSC) (UK CSC, 2025). This approach, still in development, would make a recognised professional designation a requirement for government business, similar in intent to DoD 8140 but broader in scope, applying particularly to contractors. While it offers the potential to raise standards and strengthen professional accountability, some stakeholders in the UK have expressed concern that such a model could inadvertently raise barriers to entry or limit diversity by imposing rigid licensing requirements. For Australia, the lesson may be to explore the balance between professionalisation and accessibility, ensuring that role definitions and competency standards are clear and rigorous, while still maintaining flexible onramps for diverse entrants into the cyber workforce.

Regionally, Singapore's Skills Future program is another example of a successful international initiative to build a capable cyber workforce. Singapore's SkillsFuture movement champions lifelong learning and skills mastery across all sectors, and in July 2024 a major initiative was launched: The Skills Pathway for Cybersecurity. This pathway is a structured, employer-driven pathway which guides both new entrants and midcareer

professionals toward four key entry-level roles – SOC Analyst, Incident Response & Forensics Analyst, Threat Intelligence Analyst, and Penetration Tester. These four pathways align with curated training and certification, internship and job interview opportunities. They are all supported via SkillsFuture funding mechanisms (The Straits Times, 2024).

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

Evidence from multiple international academies and training providers, including global training providers (SANS, ISC2, ISACA, CompTIA, and others), and case studies such as Rogers Cybersecure Catalyst, Maryland Cyber Workforce Academy, and WiCyS shows that practitioner-led, certification-anchored programmes consistently deliver strong outcomes. Across these models, programmes achieve approximately 80-90% placement within 12 months and 85-90% certification attainment rates.

1. WiCyS + SANS Scholarship: 92% placement of women in cyber roles within 12 months.

2. Maryland Cyber Workforce Academy: 87% employment outcomes, with an average $45k annual salary uplift (SANS, 2025).

3. Rogers Cybersecure Catalyst (Canada): 11 applicants per available position; more than 1,200 trained with strong certification attainment (Rogers Cybersecure Catalyst, 2025).

4. CyberFirst (UK, National Cyber Security Centre (NCSC)): Trains thousands of students annually through summer schools, apprenticeships, and bursaries. The UK's National Cyber Security Centre (NCSC) reports CyberFirst is a key pipeline for UK ISAC analysts and national cyber programmes. Success metrics: high participation leading to direct roles in government/industry. The program is cited by the (NCSC, 2024) as critical to staffing UK's cyber ecosystem.

5. US CyberCorps: Scholarship for Service (SFS). Since inception, more than 4,500+ graduates have been placed into US federal/state agencies. Graduates must serve in government for the same duration as their scholarship, ensuring direct employment and retention. The program has a reported average job placement rate of 95% for graduates entering cyber roles within 6 months of completion (US National Science Foundation, 2024) .

6. Corporate models: Programs including IBM apprenticeships, Airbus HR-security integration, and United Airlines' five-part talent strategy (challenge, tech stack, continuous education, exec sponsorship, unique benefits) provide examples of successful initiatives.

Key design features to embed:

1. Scholarship-to-job pipelines with employer guarantees.
2. Mentorship and reverse-mentoring (linked to higher promotion outcomes).
3. Flexible work models, career action plans, and structured rotations to prevent burnout and improve retention.
4. Evidence demonstrates that structured, intensively supported, hands-on, rapid reskilling academies with certification and employer pathways deliver the highest returns.
5. Other initiatives including AustCyber's Skills Fund, Singapore's SkillsFuture track, the EU CYBERWISER/CONCORDIA academies, and Australia's ADF Cyber Gap program are promising additions to the international ecosystem, though comparable employment and certification outcome data is not yet publicly available.

Question 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?

A range of industries provide transferable skills that map directly into high-demand cyber roles. Veterans bring crisis management and incident response expertise suited to SOC and Computer Security Incident Response Team (CSIRT) functions. Educators contribute analytical and communication strengths that translate into cyber awareness and culture leadership. Healthcare professionals demonstrate vigilance and record-keeping discipline valuable for forensics and fraud response. Engineers across mechanical, electrical and chemical disciplines offer systems knowledge and safety-first approaches well aligned to OT/ICS roles. IT and help-desk staff provide troubleshooting and administration skills that underpin SOC analysis and incident response.

Financial services, auditing, and compliance professionals bring governance, risk, and compliance expertise that transitions into cyber risk management and compliance functions. Aviation and other safety-critical sectors emphasise reliability and lifecycle risk management, paralleling secure-by-design approaches in long-term product development. Organisations such as Airbus, EY and Santander demonstrate how recruiting from teaching, military, and healthcare backgrounds has delivered adaptable professionals valued for problem-solving and resilience as much as for technical depth.

Case studies provide concrete illustrations of transferrable skill application:

1. Veterans transitioning into SOC and OT/ICS roles at IBM and US federal agencies, applying military crisis training to cyber incident response (SANS & GIAC, 2025).

2. Teachers and educators entering cyber awareness and security training roles, using pedagogy to simplify technical concepts for broad audiences (SANS & GIAC, 2025).
3. Nurses and allied health professionals retraining into DFIR and fraud analysis roles, leveraging meticulous record-keeping and situational awareness (Rogers Cybersecure Catalyst, 2023).
4. Engineers moving into OT/ICS cyber security, bringing knowledge of control systems and physical safety processes that underpin industrial security environments (SANS & GIAC, 2025).

These examples show that the strongest feeder pools are those where the underlying competencies such as communication, discipline, analytical ability, or systems engineering map directly onto the requirements of critical cyber roles.

Question 42: How can industry, academia, think tanks and government best work together to set research priorities and drive innovation?

Workforce is the bridge between research and application. Embedding workforce development into research programmes ensures that outcomes are operationalised, not just published. Pairing funded PhDs with industry placements in cyber ranges or government CERTs can produce both research outputs and job-ready talent. National workforce frameworks (NICE/ECSF) can anchor these partnerships by standardising skills definitions across academia, government and industry (Rogers Cybersecure Catalyst, 2023).

Question 43: How can government and academia enhance partnership and people-to-people links?

Structured mobility programmes are critical. Secondments, fellowships, and joint academies create 'boundary spanners' who can operate across academia, policy, and industry. The UK CyberFirst apprenticeship model demonstrates that grants tied to service placements both train talent and deepen institutional partnerships (UK NCSC, 2024). Similar co-funded placements could be scaled in Australia under Horizon 2.

Question 44: How would we best identify and prioritise sovereign capabilities for growth?

The workforce lens highlights that sovereign capability is not just about tools, but the ability to develop, operate and maintain them. Priority areas should be identified by scarcity of skills (e.g. OT/ICS, AI security, forensics), measured by time-to-fill roles (69 days for OT engineers, 79 for SOC analysts) (Rogers Cybersecure Catalyst, 2023). Sovereign capability mapping should therefore integrate labour market data with capability assessments, ensuring gaps in human capital are elevated alongside gaps in technology.

Question 45: What are the areas of most concern for ICT concentration and what mitigation is most effective?

Workforce diversification mitigates concentration risk. Over-reliance on overseas contractors or single-vendor ecosystems is compounded when skills pipelines are narrow. Incentivising domestic academies and certification programs in cloud, AI and OT security builds resilience. Case studies from Airbus and IBM show that embedding HR partners within security functions and rotating staff through SOC/OT environments produces sustainable internal pipelines (Rogers Cybersecure Catalyst, 2023).

Shield 6: Strong Region and Global Leadership

Question 47: How else could Australia engage with Southeast Asia and the Pacific?

Workforce diplomacy is the most durable tool. Scholarship-to-service models such as the US CyberCorps and UK CyberFirst prove effective at binding training to service (U.S. National Science Foundation (NSF), 2025) UK National Cyber Security Centre (NCSC), 2024). Australia could co-develop a Pacific Cyber Academy, training analysts from partner nations in OT/ICS and SOC operations while guaranteeing roles in national CERTs. This builds sovereign capacity in the region and deepens Australia's strategic ties.

Question 48: Is there additional value Cyber RAPID could provide in the region?

Yes - by adding a skills development stream. Cyber RAPID deployments could include joint training modules, mentoring, and certification pathways for host-country staff, ensuring capability uplift remains after deployments conclude. Embedding Australian-trained professionals alongside Pacific teams creates both immediate surge capacity and long-term resilience (Rogers Cybersecure Catalyst, 2023).

Question 49: In which forums and on which issues should Australia focus?

Australia should champion workforce standards and mobility in international cyber forums (e.g., ASEAN, UN, Quad). Driving alignment on frameworks such as NICE/ECSF, certification portability, and OT/AI security competencies would enable skilled professionals to move across jurisdictions, strengthening collective defence. This mirrors efforts in aviation where safety certification is internationally harmonised (Rogers Cybersecure Catalyst, 2023).

Question 50: What regulatory frameworks should be prioritised for international alignment?

Regulations increasingly embed workforce validation (NIS2, DORA, UK Cyber Bill, US DoD 8140, CMMC) (SANS & GIAC, 2025). Australia should prioritise alignment with these, particularly in requiring organisations to prove staff competence

through certifications or frameworks. This not only supports regulatory interoperability but also incentivises continuous professional development across Australia's cyber workforce.

Proportional Impact of Workforce Initiatives within Horizon 2

The workforce and capability initiatives outlined in this submission, including national academies, OT/ICS and AI specialist pipelines, certification and continuous professional development frameworks, SME training vouchers, diversity scholarships, and workforce diplomacy, represent approximately one quarter to one third of the total Horizon 2 program by the number of initiatives. Generally, these measures are relatively more resource-intensive than awareness campaigns or policy harmonization, but the ROI is disproportionately high, with workforce shortage identified as the single greatest bottleneck to resilience (ISC2, 2024; World Economic Forum, 2024; ENISA, 2022). While workforce may appear smaller on paper, it is the multiplier that enables every other Horizon 2 initiative to succeed. For this reason, workforce should be recognised as the largest enabler of Horizon 2 despite its smaller textual footprint in the consultation paper.

Conclusion

We submit that while workforce initiatives make up a smaller portion of the consultation paper by length, they are in fact the biggest enabler of Horizon 2 success. Regulatory reforms, technology deployments, and awareness programmes cannot deliver outcomes without a skilled workforce to implement and sustain them. Workforce investment is the multiplier that makes every Shield operational.

To uplift the Cyber Workforce quickly, we recommend shifting focus from headcount to skills; accelerating the delivery of the cyber workforce professionalization framework to standardise role definitions; investing in training and certification programmes, including prioritisation of critical skills roles (AI security and OT/ICS); and scaling onramps that rapidly place diverse Australians into critical cyber jobs.

Real investment into a sovereign workforce, through programmes focused on skills and competence, is the fastest way to meaningfully enhance our cyber capability. Australia is not the first nation to take action to enhance its Cyber Capability. Understanding the lessons identified globally, from other countries, enterprises, throughout the Cyber Industry, but also other professionalised industries, is key to ensuring resources are applied most effectively, and to programmes and initiatives that have proven success. To be the most cyber secure nation by 2030, Australia must leverage global partnerships and resources while investing in sovereign capabilities including workforce as a critical enabler.

Disclaimer

While SANS provides global expertise and data to inform this submission, we recognise that no single provider can meet Australia's cyber workforce needs. Horizon 2 should support a diverse ecosystem of established training and education institutions , including professional associations, international certification bodies, and public/private training providers , all of which should be accredited based on measurable outcomes such as job placements, qualifications and/or certifications earned, and workforce retention.

References

Australian Signals Directorate (ASD)- ACSC . (2024). Annual Cyber Threat Report 2023-2024. https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024

CSA Singapore (CSA SG). (2025). 11 Critical Sectors Come Together to Tackle Complex Cyber Threat Scenarios in National Cyber Crisis Management Exercise. https://www.csa.gov.sg https://www.csa.gov.sg/news-events/press-releases/11-critical-sectors-come-together-to-tackle-complex-cyber-threat-scenarios-in-national-cyber-crisis-management-exercise

Electricity – Information Sharing and Analysis Centre (EISAC). (2025) About the EISAC, https://www.eisac.com/s/about-the-eisacISC2. (2024). Cybersecurity Workforce Study. https://www.isc2.org/Research

European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive)

https://eur-lex.europa.eu/eli/dir/2022/2555/

European Union Agency for Cybersecurity (ENISA). (2022). ENISA supports the cooperation among sectorial Information Sharing and Analysis Centres (ISACs): https://www.enisa.europa.eu/news/enisa-supports-the-cooperation-among-sectorial-information-sharing-analysis-centers-isacs

European Union Agency for Cybersecurity (ENISA). (2022). Cross Sector Exercise Requirements. https://www.enisa.europa.eu/publications/cross-sector-exercise-requirements

NICE (NIST). (2020). National Initiative for Cybersecurity Education (NICE) Workforce Framework https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center

Rogers Cybersecure Catalyst. (2023). 5 years of Impact 2018-2023. https://cybersecurecatalyst.ca/impact/

SANS Institute (2025). Cyber Skills Shortage: SANS Institute to Triple Academy Cybersecurity Scholarships By 2026,https://www.sans.org/blog/cyber-skills-shortage-sans-institute-to-triple-academy-cybersecurity-scholarships-by-2026

SANS Institute & GIAC (2025). Cybersecurity Workforce Research Report. Global Skills, Validation, and Hiring Trends. https://www.sans.org/mlp/2025-attract-hire-retain-cybersecurity-roles

Saudi National Cybersecurity Authority - Public Awareness Campaigns. https://nca.gov.sa/en/cyber-awareness/

The Straits Times. (2024). New skills pathway into the cyber security field launched for new entrants, mid-careerists. Retrieved August 28, 2025, from https://www.straitstimes.com/singapore/new-skills-pathway-into-the-cyber-security-field-launched-for-new-entrants-mid-careerists

United Arab Emirates (2024) Cyber Safety https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security/cyber-safety#:~:text=%27Cyber%20Pulse%27%20initiative,The%20second%20phase%20targeted%20students.&text=Web%20users%20should%20not:,any%20apps%20from%20unknown%20sources

UK Cyber Security Council (2025) Chartered Status Framework: https://www.ukcybersecuritycouncil.org.uk/careers-and-learning/cyber-career-framework/

UK National Cyber Security Centre (NCSC). (2024). CyberFirst Programme. Retrieved from https://www.ncsc.gov.uk/cyberfirst

US Department of Defence. (2023). DoD 8140 Cyberspace Workforce Framework. https://dodcio.defense.gov/Cyber-Workforce/DCWF.aspx

U.S. National Science Foundation (NSF). (2025). CyberCorps®: Scholarship for Service (SFS). Retrieved from https://www.sfs.opm.gov

U.S. National Science Foundation (NSF). (2024) 2024 SFS Biennial report https://www.nsf.gov/funding/opportunities/sfs-cybercorps-scholarship-service/updates/105530

World Economic Forum (WEF). (2024). Strategic Cybersecurity Talent Framework. https://www.weforum.org/publications/strategic-cybersecurity-talent-framework/

Women in Cybersecurity (WiCyS). (2025). Skills Development Training Programs. https://www.wicys.org/initiatives/programs/

World Economic Forum, 2025, 'The power of partnership: How the UAE is securing cyberspace' www.weforum.org/stories/2025/06/uae-securing-cyberspace/

Additional References

ISACA. (2024). State of Cybersecurity 2024: Global Update on Workforce, Resources and Budgets. https://www.isaca.org/resources/reports/state-of-cybersecurity-2024

CompTIA. (2025). Workforce and Learning Trends 2025. https://www.comptia.org/en/resources/research/workforce-and-learning-trends-2025/

OECD. (2023). Building a Skilled Cyber Security Workforce in Five Countries . https://www.oecd.org/en/publications/building-a-skilled-cyber-security-workforce-in-five-countries_5fd44e6c-en.html