SUBMISSION

Submission to the Department of Home Affairs

Submission on developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy

29 August 2025

The Australian Academy of Technological Sciences and Engineering (ATSE) is a Learned Academy of independent, non-political experts helping Australians understand and use technology to solve complex problems. Bringing together Australia's leading thinkers in applied science, technology and engineering, ATSE provides impartial, practical and evidence-based advice on how to achieve sustainable solutions and advance prosperity.

Robust cyber security underpins social resilience and national security. As digital technologies become increasingly pervasive and interconnected, the risk and impact of cyber threats grow. Cyber security threats are becoming more frequent and more complex, with the potential to disrupt essential services and critical infrastructure, threaten sensitive data, and economically impact Australian businesses.

Addressing these challenges requires greater investment in research and development (R&D) for cyber security, particularly for emerging technologies that support critical infrastructure in core sectors including water, energy, health and transport. Additionally, the adoption of a shared language to strengthen industry collaboration and threat detection ability is important to identify and tackle emerging threats. Efforts to mitigate cyber security skill shortages can also be made through increased access to upskilling and reskilling opportunities, including microcredentials and short courses. Finally, existing cyber security campaigns can be adapted to reach children and teenagers, building their lifelong cyber safety skills and increasing cyber security resilience in the long-term.

ATSE makes the following recommendations to inform Horizon 2 of the 2023-2030 Australian Cyber Security Strategy:

Recommendation 1: Uplift in R&D across the economy, including in cyber security for emerging technologies in critical infrastructure.

Recommendation 2: Strengthen global partnerships in cyber security to foster joint R&D and build resilience against cross-border threats.

Recommendation 3: Continue supporting the development of the National Voluntary Data Classification Framework, aiming for universal adoption if proven effective.

Recommendation 4: Target the cyber security skills gaps across the workforce by promoting and expanding cyber security microcredentials, short courses, and professional development, prioritising access for Small and Medium Enterprises (SMEs).

Recommendation 5: Expand and update cyber security awareness campaigns, including the Act Now, Stay Secure Campaign, to children and teenagers, including by leveraging existing evidence-based resources.

Investing in R&D to secure critical infrastructure and national resilience

Robust cyber security is essential for Australia's critical infrastructure as it becomes increasingly digitised and distributed: energy and water are distributed through Supervisory Control and Data Acquisition (SCADA) systems, health care is adopting electronic prescribing and digital records, transport is incorporating semi-autonomous vehicles, and defence capabilities are increasingly reliant on technological innovation (Karl and Schell 2024; AIHW 2024; NSW Government 2022; Department of Defence 2024).

Critical infrastructure can be a prime target for a cyberattack. For example, Ukraine faced a coordinated cyberattack on three regional electrical power distribution companies in 2015, leading to power outages affecting 225,000 customers (Ratnam et al. 2020). The largest water company in the United States, American Water, was targeted by a cyberattack in 2024, leading to the disconnection of key systems including customer-facing services (Reed 2024). Cyberattacks have the potential to destabilise affected regions, producing both online and real-life consequences. Despite the potential disastrous effects of a cyberattack, many systems within critical infrastructure are not designed with cyber security in mind. The rise of the Internet of Things (IoT), increased reliance on real-time data, and the mounting threat of quantum decryption are leading to a greater number of potential access points vulnerable to cyberattack (Ratnam et al. 2020; Van der Schyff 2025). Investing in existing and new cyber security systems and technologies, including AI and machine learning threat detection, cloud security and IoT security, could help prepare for future cyber threats including for critical infrastructure (Gov UK 2025). ATSE recommends an uplift in R&D across the economy, including in cyber security for emerging technologies in critical infrastructure. This uplift is important to secure core sectors such as water, energy, health, transport and defence.

Australia also has an opportunity to strengthen global partnerships in research to support cyber security resilience. Cyberattacks often do not obey traditional borders, emphasising the importance of R&D coordination and collaboration with neighbouring countries and global allies (Kleijssen and Perri 2017). ATSE recommends strengthening existing partnerships within the Pacific and Southeast Asia to continue capacity building in the region. Additionally, Horizon Europe offers an opportunity for Australia to strengthen global partnerships for R&D

outside of the region, including with specific funding invested into cyber security initiatives (European Research Executive Agency 2025).

Recommendation 1: Uplift in R&D across the economy, including in cyber security for emerging technologies in critical infrastructure.

Recommendation 2: Strengthen global partnerships in cyber security to foster joint R&D and build resilience against cross-border threats.

Strengthening industry coordination in cyber security

Industry plays a crucial role in Australia's cyber security efforts through ownership of critical infrastructure, innovation in emerging technologies, and maintenance of supply chain security. Effective cooperation and communication are essential for industry to work collaboratively and with government. This is particularly important under the Security of Critical Infrastructure Act 2018 (SOCI) and the recent introduction of the Risk Management Program, which requires Responsible Entities to submit annual reports demonstrating the implementation of robust risk management frameworks. The National Voluntary Data Classification framework, in development by the Department of Home Affairs and CSIRO's Data61, offers a way to increase collaboration through the adoption of a shared language when discussing data and cyber security (Department of Home Affairs and CSIRO 2025). This shared language can increase the effectiveness of industry's threat reporting ability and the efficiency of programs, including the SOCI Act's Risk Management Program. If the framework is shown to improve security controls, data governance and customer trust, universal implementation of the framework should be considered.

Recommendation 3: Continue supporting the development of the National Voluntary Data Classification Framework, aiming for universal adoption if proven effective.

Increasing cyber security upskilling and reskilling opportunities

The cyber security industry is facing a persistent and significant shortfall of an estimated 30,000 skilled workers, amidst broader skills shortages across the economy (Braue 2024). Over 80% of Australian organisations experienced a cyberattack in 2023 alone and breaches are continuing to rise (Penn 2023; Office of the Australian Information Commissioner 2024). Small and Medium Enterprises (SMEs) are particularly at risk, with 43% of cyberattacks aimed at small businesses. On average, SMEs experience more significant losses due to cyberattacks than large businesses and spend less on cyber security measures (Export Finance Australia 2023). With human factors being central to the effectiveness of cyber security, maintaining a highly skilled and up-to-date workforce of sufficient size is essential to sustained cyber resilience.

While Australia has a number of traditional university and vocational pathways, these alone are unlikely to deliver the graduates required to fill the skills gap (D'Rosario 2022). Short-term training and qualifications delivered by academia and industry can upskill or reskill both cyber security graduates and employees from other fields (D'Rosario 2022). Microcredentials and short courses can provide targeted, adaptable training that can be integrated into existing qualifications or used as stand-alone certificates (Galindo 2023). Collaboration between industry and academia can assist in ensuring these programs keep pace with emerging threats and knowledge gaps. Increasing the promotion and development of cyber security microcredentials, short courses, and professional development to upskill or reskill workers would help increase the domestic talent pool. Access to these courses should be prioritised for SMEs due to their heightened vulnerabilities to cyber threats and lower rates of cyber security competency. By expanding rapid training options, Australia can modernise and build its domestic talent pool – one equipped to protect businesses and critical infrastructure and reduce systemic vulnerabilities.

Recommendation 4: Target the cyber security skills gaps across the workforce by promoting and expanding cyber security microcredentials, short courses, and professional development, prioritising access for Small and Medium Enterprises (SMEs).

Expanding cyber security awareness for young Australians

Young people are particularly vulnerable to online risks, and as technologies and their risks continue to evolve, education and awareness initiatives must adapt. It is especially important to promote cyber security messaging aimed at young people in the changing regulatory environment around online safety. The implementation and effects of the upcoming Children's Online Privacy Code and Social Media Age Restrictions are examples of topics intersecting with cyber security that can be communicated to children and teenagers through campaigns. Campaigns, including the Department of Home Affairs' *Act Now Stay Secure* campaign, delivered as part of Horizon 1 of the 2023 – 2030 Australian Cyber Security Strategy, can be expanded to target under 18-year-old Australians more effectively as the Strategy moves to Horizon 2. Some existing evidence-based resources for online safety could be leveraged for a campaign, such as the Cyber Safety Project. Embedding cyber security education into youth-focused initiatives will not only support children and teenagers to stay safe but will also improve resilience to cyber threats in the long term as they enter tertiary education and the workforce.

Recommendation 5: Expand and update cyber security awareness campaigns, including the Act Now, Stay Secure Campaign, to children and teenagers, including by leveraging existing evidence-based resources.

ATSE thanks the Department of Home Affairs for the opportunity to respond to Horizon 2 of the 2023-2030 Australian Cyber Security Strategy. For further information, please contact academypolicyteam@atse.org.au.

References

Australian Department of Defence (2024) *Defence Innovation, Science and Technology Priorities*, https://www.defence.gov.au/sites/default/files/2024-09/Defence-IST-Priorities_0.pdf, accessed 19 August 2025.

Australian Institute of Health and Welfare (2024) *Digital Health*, *Australia's Health*, https://www.aihw.gov.au/reports/australias-health/digital-health#:~:text=Digital%20health%20innovation%2C%20including%20telehealth,planning%20and%20optimise%20resource%20allocation., accessed 18 August 2025.

Braue D (2024) *Australia's 'miniscule' cyber workforce won't cut it*, *ACS Information Age*, https://ia.acs.org.au/article/2024/australia-s--miniscule--cyber-workforce-won-t-cut-it.html, accessed 19 August 2025.

Department of Home Affairs and CSIRO (2025) 'Voluntary Data Classification Framework', https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/technology-and-data-security/voluntary-data-classification-framework, accessed 19 August 2025.

D'Rosario M (2022) *Upskilling and Expanding the Australian Cyber Security Workforce*.

European Research Executive Agency (2025) *Horizon Europe - Cluster 3: 'Civil security for society'*, https://rea.ec.europa.eu/funding-and-grants/horizon-europe-cluster-3-civil-security-society_en, accessed 19 August 2025.

Export Finance Australia (2023) *Australia - Small businesses vulnerable to rising cybercrime*, https://www.exportfinance.gov.au/resources/world-risk-developments/2023/march/australia-small-businesses-vulnerable-to-rising-cybercrime/, accessed 19 August 2025.

Galindo M (2023) *Making Macro Impact: How Micro-credentials are Shaping a Skills-based Economy*.

Gov UK (2025) *Emerging technologies and their effect on cyber security*, https://www.gov.uk/government/publications/emerging-technology-pairings-and-their-effects-on-cyber-security/emerging-technologies-and-their.

Karl M and Schell D (2024) 'Why SCADA modernization is a priority for water utilities', Australian Water Association, Accessed 18 August 2025, https://www.awa.asn.au/resources/latest-news/why-scada-modernisation-is-a-priority-for-water-utilities#:~:text=Supervisory%20Control%20and%20Data%20Acquisition,in%20such%20a%20complex%20migration., accessed 18 August 2025.

Kleijssen J and Perri P (2017) 'Cybercrime, evidence and territoriality: Issues and options', In *Netherlands Yearbook of International Law*, T.M.C. Asser Press, doi:10.1007/978-94-6265-207-1_7.

NSW Government (2022) *Connected and Automated Vehicles Plan*, https://www.future.transport.nsw.gov.au/sites/default/files/2022-06/connected_and_automated_vehicles_plan.pdf, accessed 18 August 2025.

Office of the Australian Information Commissioner (2024) *Notifiable data breaches report January to June 2024*, https://www.oaic.gov.au/__data/assets/pdf_file/0013/242050/Notifiable-data-breaches-report-January-to-June-2024.pdf, accessed 19 August 2025.

Penn C (2023) *2023 Cybersecurity Skills Gap*.

Ratnam EL, Baldwin KGH, Mancarella P, Howden M and Seebeck L (2020) 'Electricity system resilience in a world of increased climate change and cybersecurity risk', *Electricity Journal*, 33(9), doi:10.1016/j.tej.2020.106833.

Reed J (2024) *Cyberattack on American Water: A warning to critical infrastructure*, *IBM*, https://www.ibm.com/think/news/cyberattack-on-american-water-warning-critical-infrastructure, accessed 21 August 2025.

Van der Schyff J (2025) *Decrypting tomorrow's threats: critical infrastructure needs post-quantum protection today*, *The Strategist - Australian Strategic Policy Institute*.