HawkerBritton
Government Relations Strategy

Cyber Security Strategy

On the 22nd of November, 2023 Cyber Security Minister Clare O'Neil released the 2023-2030 Cyber Security Strategy (The Strategy) available here.

In addition to the $2.3 Billion of existing initiatives, the Government has committed $586.9 million to implement the goals outlined in the Strategy. This includes:

- $290.8m including support for small and medium businesses, building public awareness, fighting cybercrime, breaking the ransomware business model, and strengthening the security of Australians' identities.
- $4.8m to establish consumer standards for smart devices and software.
- Uplifting the cyber security of Australia's health system by investing $9.4m to build a threat-sharing platform for the health sector.
- Defending Australia's critical infrastructure by investing $143.6m to strengthen Australia's critical infrastructure protections and uplifting government cyber security.
- Growing Australia's sovereign cyber capabilities by investing $8.6m in professionalising our cyber workforce and accelerating the cyber industry in Australia.
- Building regional cyber resilience and global leadership by investing $129.7m in regional cooperation, cyber capacity uplift programs, and leadership in cyber governance forums on the international stage.

The strategic plan delineates six cyber shields designed to safeguard Australian businesses and citizens from cyber threats. The reforms under each shield have been summarised below.

Shield 1 - Strong businesses and citizens

- Create cyber 'health checks' for small and medium businesses
- Establish a Small Business Cyber Security Resilience Service
- Expand the national cyber security awareness campaign
- Fund grants to community organisations
- Amplify current cybercrime disruption activities
- Drive global cooperation to effectively prevent, deter and respond to cybercrime
- Build regional capabilities to fight cybercrime
- Work with industry to co-design options for a mandatory no-fault, no-liability ransomware reporting obligation
- Create a ransomware playbook to provide further guidance to businesses on how to prepare for, deal with and bounce back from a ransomware or cyber extortion attack.
- Leverage Australia's role in the Counter Ransomware Initiative.
- Provide industry with additional information on cyber governance obligations under current regulations.
- Establish a Cyber Incident Review Board to conduct no-fault incident reviews.

- Develop a single reporting portal for cyber incidents.
- Consult industry on options to establish a legislated limited-use obligation.
- Co-design a code of practice for cyber incident response providers.
- Expand the Digital ID program.
- Expand support services for victims of identity theft.

Shield 2 - Safe Technology

- Adopt international security standards for consumer-grade smart devices.
- Co-design a voluntary labelling scheme to measure the cyber security of smart devices.
- Co-design a voluntary cyber security code of practice for app stores and app developers.
- Work with Quad partners to harmonise software standards for government procurement.
- Develop a framework for assessing the national security risks.
- Conduct a review to identify and develop options to protect Australia's most sensitive and critical data sets.
- Review Commonwealth legislative data retention requirements.
- Review the data brokerage ecosystem.
- Work with industry to design a voluntary data classification model.
- Embed cyber security into our work on responsible AI to help ensure that AI is developed and used safely and responsibly.
- Set standards for post-quantum cryptography.

Shield 3 - World-class threat sharing and blocking

- Establish the Executive Cyber Council as a coalition of government and industry leaders.
- Continue to enhance ASD's existing threat-sharing platforms.
- Launch a threat-sharing acceleration fund.
- Encourage and incentivise industry to participate in threat-sharing platforms.
- Work with industry to pilot next-generation threat-blocking capabilities across Australian networks.
- Encourage and incentivise threat blocking across the economy.

Shield 4- Protected critical infrastructure

- Align telecommunication providers to the same standards as other critical infrastructure entities.
- Clarify the regulation of managed service providers under the SOCI Act.
- Explore options to incorporate cyber security regulation as part of expanded 'all hazards' requirements for the aviation and maritime sectors.
- Protect the critical data held, used and processed by critical infrastructure.
- Activate enhanced cyber security obligations for Systems of National Significance.
- Finalise a compliance monitoring and evaluation framework.

- Expand crisis response arrangements to ensure they capture secondary consequences from significant incidents.
- Enable the National Cyber Security Coordinator to oversee the implementation and reporting of cyber security uplift.
- Develop a whole-of-government zero-trust culture.
- Conduct regular reviews of the cyber maturity of Commonwealth entities.
- Designate 'Systems of Government Significance' that need to be protected with a higher level of cyber security.
- Uplift the cyber skills of the Australian Public Service.
- Expand the National Cyber Exercise Program.
- Develop incident response playbooks.

Shield 5 - Sovereign Capabilities

- Grow and expand Australia's cyber skills pipeline.
- Provide guidance for employers to target and retain diverse cyber talent.
- Build a framework for the professionalisation of the cyber workforce.
- Provide cyber start-ups and small-to-medium enterprises with funding to develop innovative solutions to cyber security challenges.

Shield 6 - Resilient region and global leadership

- Refocus Australia's cyber cooperation efforts.
- Build a regional cyber crisis response team.
- Pilot options to use technology to protect the region at scale.
- Collaborate with partners in international standards development forums.
- Advocate for high-quality digital trade rules.
- Continue to defend an open, free, secure and interoperable internet in international forums.
- Continue to uphold and improve the framework of responsible state behaviour in cyberspace
- Increase costs for malicious cyber actors.

Next Steps

Alongside the Strategy, the Government will shortly release a Consultation Paper to work directly with industry to inform proposed legislative reform on:

- new initiatives to address gaps in existing laws
- amendments to the Security of Critical Infrastructure Act 2018 to strengthen protections for critical infrastructure.

When released, further information on the consultation will be available here.

The consultation period will run until March 2024.

For more information, please contact Hawker Britton's Director Emma Webster at ewebster@hawkerbritton.com