2023-2030 Australian Cyber Security Strategy Discussion Paper

Victorian Government Submission

May 2023

Introduction

The Victorian Government plays a key role in protecting government systems against cyber-attacks, as well as supporting private industry and the community to be resilient to the challenges of the digital world. Technology is now a major part of most of our lives. We depend on it for essential services, information, connection and entertainment. We spend our time online and trust devices with sensitive information.

Government, industry and the community face constant threats from cyber criminals, organised crime groups, online vandals, trusted insiders, advanced persistent threat groups and foreign governments.

Victoria welcomes the opportunity to contribute to the development of the 2023-2030 Australian Cyber Security Strategy.

Victoria's Cyber Strategy Approach

Victoria's Cyber Strategy 2021 sets the Victorian Government's cyber agenda for the next five years. It defines long-term objectives and provides the framework for an annual Mission Delivery Plan setting out our priorities.

Victoria's Cyber Strategy 2021 is delivered through three core missions:

1. The safe and reliable delivery of government services. Mission 1 strengthens the defences of Victorian Government networks and services to meet equal to current and emerging threats. This mission protects the confidentiality and integrity of sensitive information and support the reliable delivery of IT-dependent government services to the Victorian community.
2. A cyber safe place to work, live and learn. Mission 2 supports individuals, households, businesses and community groups to connect, engage and work safely online. This mission aligns community engagement, education, legislation, policing and emergency management arrangements to foster a cyber resilient culture for Victoria.

3. A vibrant cyber economy. Mission 3 develops strategic partnerships to grow a dynamic and competitive cyber sector underpinning digital transformation, growth and innovation across every sector of the Victorian economy. The mission presents opportunities for local job creation, foreign direct investment and to improve cyber skills and expertise. These actions position Victoria as a global leader in cyber risk management and support the state's economic prosperity.

Victoria cooperates heavily with the Commonwealth Government and other jurisdictions to manage cyber security as a state significant risk. Victoria thanks the Commonwealth for its ongoing contribution and support to keep Victoria cyber safe.

The safe and reliable delivery of government services

Australia continues to be the target of persistent cybercrime and espionage by a wide range of criminal and state actors, including foreign intelligence services, seeking information on political, diplomatic, military, and personal data.

The discussion paper acknowledges the Commonwealth Government controls and processes some of Australia's most sensitive data to deliver essential public services and must continue to invest into hardening these systems against cyber risk.

However, the discussion paper is largely silent on the cyber security risk to State and Territory Governments, which deliver most frontline and essential services to the community, while also holding significant volumes of sensitive community data.

States and Territories play a critical role in managing cyber security incidents and consequences of essential services, including electricity, gas, liquid fuels, water and communications. It is important to recognise that State Ministers and their departments operate within State emergency management frameworks and operate within statutory roles related to these services.

Supporting the Australia Government to become cyber safe

Victoria proposes that if the 2023-2030 Australian Cyber Security Strategy intends to achieve its vision of making Australia the most cyber safe nation by 2030, further financial, technical and operational support must be provided to State and Territory governments. This includes:

a. enhanced real-time and strategic intelligence sharing from the Commonwealth Government on cyber security threats to public sector organisations
b. Commonwealth funding being made available to protect the essential services states deliver from malicious cyber-attacks from highly resourced threat groups, in particular those associated with foreign governments.
c. enhanced operational cooperation to improve real time responses to cyber threats, incidents and emergencies
d. technical support to prevent threats from reaching public sector IT networks – i.e., 'blocking threats at the digital border'
e. increased support to adopt basic cyber security controls, such as the Essential Eight Maturity Model

f. establishing a national vulnerability disclosure program enabling researchers to highlight exploitable and prioritised vulnerabilities to a central body and alert organisations and government bodies to potential indicators of compromise. This should be a funded program that awards researchers on issues impacting critical infrastructure
g. establishing a national cloud services registry ensuring all cloud-based service providers offering platform services into Australia have been assessed against Australian Privacy requirements and the security standards of the Protective Security Policy Framework
h. addressing the cyber skills shortage across governments by making it easier for cyber security professionals to move between jurisdictions.

Any obligation of confidentiality upon the Australian Signals Directorate (ASD), Australian Cyber Security Centre (ACSC), engaging organisations which experience a cyber incident needs to consider the potential implications on the Cyber Incident Management Arrangements (CIMA) for Australian Governments. An obligation of confidentiality may hamper cyber incident response, consequence management and undermine the State regulatory powers through preventing information flow to key response agencies.

Increasing benefits through cooperation

As the cyber threat continues to grow, increasing our operational cooperation through the establishment of joint teams, similar to our shared approach to counter terrorism, will reduce barriers to collaboration and keep critical infrastructure safe.

Victoria has robust critical infrastructure resilience arrangements in place, via legislation and policy, that provide a framework for collaboration, information sharing, and building sector or organisational resilience across all hazards. Victoria is actively considering the threat of cyber risk to our critical infrastructure network and any enhancements to arrangements that may be required.

Victoria encourages strong cooperation between the Commonwealth Government and all jurisdictions in the development and delivery of national initiatives under the 2023-2030 Australian Cyber Security Strategy. Cooperation and open channels of communication will increase the benefits for Australia, the community and economy.

A cyber safe place to work, live and learn

The community and economy are under persistent attack from cybercriminal groups seeking to profit from cyber harm. The discussion paper identifies ransomware and associated extortion threats, espionage and fraud as a significant threat to the public sector and Australian organisations. It also highlights the importance of improving national responses to these risks, including by potentially prohibiting payment of cyber ransoms and extortions.

Australians should have confidence that digital products and services sold are fit for purpose and include appropriate best practice cyber security and personal information protections. Various jurisdictions, including the Commonwealth Government, have previously discussed the concept of a community facing 'star rating system' to identify the cyber security safety level of technology products.

Making it easier for consumers to make cyber informed decisions would reduce cyber harm from impacting the community.

Victoria also encourages the Commonwealth Government to consider the impact a cyber-attack can have on a person's physical safety. This threat is real and present, particularly in relation to infrastructure services, such as transport, and should be considered an important element when developing the 2023-2030 Australia's Cyber Security Strategy.

Collaborative efforts towards regulation reform

The discussion paper identifies enhancing and harmonising regulatory frameworks as a priority for improving Australia's national cyber resilience. Australians should have confidence that services used and sold are fit for purpose and include appropriate best practice cyber security protections improving outcomes for the community and economy. Australians should also be protected from potential physical harm resulting from cyber-attacks.

Victoria strongly suggests that any legislative or regulatory reforms should avoid undue regulatory burden, recognise the States and Territories as regulators of essential services and provide appropriate practical guidance and implementation tools. In particular, any further reform to the *Security of Critical Infrastructure Act 2018* (Cth) should be undertaken in consultation with the States and Territories.

In addition, Victoria recommends that any reform is developed in partnership with the cyber, privacy and information management sector. To limit harm from data breaches, any regulation reform should require collected personal or sensitive data to be actively managed and disposed of when it is no longer required.

Being a clear and trusted voice for the community

Co-developed and delivered community initiatives, such as awareness campaigns, can reduce the likelihood and impact of damaging cyber-attacks on the community and economy. Establishing a clear and trusted voice to the community on cyber security is a priority for Victoria, including to its diverse community groups. Victoria is focused on improving community resilience through schools, community programs and business outreach programs and would welcome the opportunity to deliver more co-developed initiatives with the Commonwealth Government.

Supporting Australia's local cyber industry

The 2023-2030 Australian Cyber Security Strategy should actively consider the challenges and needs of small-to-medium sized enterprises (SMEs) to ensure the impacts of regulation reform are considered appropriately. For the Australian cyber sector to be a world-leader in creating innovative products, the sector must be agile to meet the evolving demands of the cyber risk environment. Legislative or regulatory reform should be flexible and responsive to evolving cyber risk while protecting sensitive and personal data of Australians.

Addressing the challenge to boost SME's cyber security awareness, resilience and capabilities across all industries is a key focus area for the Victorian Government under Missions 2 and 3 of Victoria's Cyber Security Strategy 2021. Supporting SMEs to become cyber resilient is also important to underpin broader resilience across industry and government supply chains. Equipping SMEs with affordable and accessible risk-mitigation tools and strategies will be key to safeguarding the

economic growth of SMEs and the broader cyber sector. It will also be critical that SMEs are provided with easy to understand, accessible and up-to-date information, education and advice on how to identify and mitigate cyber security-risks.

To uplift capability and reduce duplication, there is an opportunity to house tailored SME-suitable cybersecurity and information management resources centrally. These resources could be made accessible through existing and established channels in each state, such as Victoria's Business Victoria website.

Consideration should be given to accessible training, workshops and other support services to continually enhance the digital literacy of SMEs, the community, and students including those from regional areas and culturally and linguistically diverse cohorts.

There is a need for accessible assistance for SMEs to help them navigate available pathways after experiencing a cyber-attack, especially after using third party marketplaces. This is particularly relevant as cyber insurance is financially out of reach for many small business owners. Further support to the community and SMEs could be explored through engaging with the technology industry to rebalance the responsibility to defend cyberspace.

Ongoing national engagement and cooperation to combat cybercrime and support policing responses is essential to support effective investigations and victim support. Building on existing cooperation between jurisdictions law enforcement engages should be reflected within the strategy.

Victoria encourages developing co-designed approaches to reduce the likelihood and impact of damaging cyber-attacks on government, industry and the community ahead before introducing deterrence measures.

A vibrant cyber economy

The growth of innovative, competitive local cyber security businesses and advanced skills capability is essential to securing Australia's economy, reducing the community impact and harm associated with cybercrime. The rapid growth of the cyber economy also presents a significant opportunity for the national economy. Capturing opportunities in cyber could create thousands of skilled, high-value job opportunities over the next few years, adding to the almost 27,000 workers currently employed in Australian cyber security roles.

Victoria notes that several potential action areas are flagged in the discussion paper and recommends that the following areas should be prioritised:

- supporting the cyber security workforce and talent pipeline
- building SME cyber resilience
- investing in the cyber security ecosystem (i.e. building scale and capability in the local sector)
- designing and sustaining cyber security in new technologies (including artificial intelligence (AI) and quantum computing).

Leveraging government procurement

Government procurement plays a significant role in encouraging the growth of Australia's cyber firms and creates partnerships with world-leading international

cyber firms. Governments can support the Australian cyber sector to be a trusted world-leader in cyber products and services by becoming early adopters of local innovations. Unfortunately, feedback from industry stakeholders indicates that some local cyber security firms are finding it easier to enter overseas markets than domestic supply chains. There is opportunity for the Commonwealth to establish a consistent approach to supply chain security across all jurisdictions which will support greater security outcomes for governments, improve economic resilience and make it easier for organisations to do business with government.

Developing a future cyber security workforce

There is opportunity to develop the cyber security profession, including technical and non-STEM roles, to ensure it meets Australia's current and future needs. The Commonwealth, in collaboration with jurisdictions, could explore more opportunities to ensure cyber security providers have the skills and knowledge necessary to support their customers. Continuing to develop the cyber workforce will support Australia's efforts to become the most cyber secure nation.

Victoria is well placed to lead the development of the national cyber security skills, talent and business pipeline. Melbourne's world-class TAFE and university sector is a driving force of business growth and innovation, with a skill-base deeper than anywhere else in Australia. Victoria produces highly skilled talent from a diverse range of world-class institutions, including Monash University, La Trobe University, Victoria University, Deakin University, RMIT University, Swinburne University of Technology, Federation University and University of Melbourne. As the gateway to Victoria's digital ecosystem, the Cremorne Digital Hub also provides a key channel to uplift the cyber capability of businesses and build a stronger cyber workforce.

In addition, Victoria has several international bilateral cyber security relationships that could be leveraged to support the strategy's ambitious vision. Victoria has built bilateral cyber security relationships through several successful initiatives:

- A Memorandum of Understanding (MoU) between the State of Victoria and SIBAT, the International Defence Cooperation Directorate of the Israel Ministry of Defence (2022). The MoU aims to foster sector capacity building and trade relations between Victorian and Israeli defence, aerospace and cybersecurity sectors.
- An MoU between Victoria's Swinburne University of Technology and Tel Aviv University (2016) that encourages research exchange with a focus on privacy, security and data analytics. scale.
- A MoU with the Commonwealth of Virginia, USA (2016) that facilitates information sharing and the safeguarding of the digital economy.

Promoting cyber career pathways

The Mission 3 Expert Advisory Panel (EAP) was established to provide insight on current and future cyber capability uplift opportunities and digital economic growth. Members include leaders from across Victoria's cyber sector, digital industries and associations, university sector and Victorian Government cyber security leaders. Advice from the EAP indicate that significantly more needs to be done to ensure the cyber sector has the necessary skills and workforce (foundation to mid-career and senior leadership levels), to realise the aspirations of the sector.

Victoria, as population, economic and business centre for Australia, presents the Commonwealth with an ideal investment location for initiatives within the strategy.

The EAP identified several opportunities that could be led at a Commonwealth level to encourage stronger cyber skills and career pathways:

- Create an interdisciplinary approach in university and TAFE programs to develop more rounded cyber skills, including both business and non-technical skillsets.
- Support upskilling and reskilling, particularly for people with existing broader Information Communications Technology (ICT) skillsets and experience.
- Raise awareness of cyber roles by targeting cyber career advice and initiatives to different and diverse cohorts, including graduates and mid-late career transitions.
- Create initiatives to improve the work-readiness of cyber graduates, including through Work Integrated Learning (WIL).
- Establish incentives and support to, employers to enable them to offer placements for cyber graduates and mid-career workers transitioning into cyber.
- Create initiatives which improve the support to students and mid-career professions to develop cybersecurity skills and knowledge.

Government initiatives to support Australia's cyber security workforce through education, skilled migration, and accreditation should be co-created with industry, education providers and state and territory governments. Victoria is supportive of skilled migration settings that attract highly skilled cyber workers to move to Australia to fill immediate skill shortages.

Compounding Australia's workforce issues is that cyber is not effectively attracting and retaining women. Although gender diversity is demonstrated to improve cyber security outcomes for businesses, women comprise just 26 per cent of the Australian cyber workforce. The 2023-2030 Australian Cyber Security Strategy should include initiatives to improve the diversity of the cyber workforce, particularly to boost the participation of women in cyber careers and leadership roles.

Conclusion

The Victorian Government plays a key role in protecting government services against cyber-attacks, as well as supporting private industry and the community to be resilient to the challenges of the digital world.

The Victorian Government welcomes the opportunity to provide further input to the development of the 2023-2030 Australian Cyber Security Strategy and assist Australia to become a global cyber leader.

It is proposed that by adopting Victoria's recommendations, the Commonwealth will be acknowledging the important role played by States, Territories and industry in protecting government, the community and economy.