2025 CISO Annual Statement: Delivering Victoria’s Cyber Strategy

This is the third annual statement by the Victorian Government Chief Information Security Officer (CISO) on the government’s progress on Victoria’s Cyber Strategy 2021.

There is a link to download a copy of this report below.

# Delivering a Cyber Safe Victoria

The cyber threat environment in Australia continues to grow in scale and complexity. The Australian Signals Directorate’s (ASD) Cyber Threat Report 2023-2024 highlighted that Australian’s reported over 87,400 cybercrimes – a reported crime every 6 minutes. Cyber criminals are also adapting new technologies such as Generative Artificial Intelligence (AI) to enhance their existing capabilities.

At the same time, cyber threat actors, including state actors, continue to target Australian critical infrastructure. In the 2025 Australian Security Intelligence Organisation (ASIO) threat assessment, the Director General of Security noted that, “cyber units from at least one nation state routinely try to explore and exploit Australia’s critical infrastructure networks”.

Since 2021, the Victorian Government has invested more than $130 million in Victoria’s cyber capabilities to improve our digital defences and enhance the state’s digital resilience. This includes $37.5 million over three years in the 2025-26 State Budget to continue Victoria’s program of cyber security activities for Victorian Public Sector organisations.

Victoria’s Cyber Strategy sets the government’s vision for creating a cyber safe Victoria. We are delivering on its three core missions:

* improving the safe and reliable delivery of government services
* creating a cyber safe place to work, live and learn
* supporting a vibrant cyber economy.

**Reducing the risk of adverse cyber security events on government systems and services**

The Department of Government Services (DGS) continues to reduce the risk of adverse cyber security events by delivering expert cyber incident response, cyber threat intelligence, consequence management and coordination services. Across 2024-25 this included:

* leading Victoria’s response to national cyber security incidents, including working with the Australian Cyber Security Centre and the Department of Home Affairs to minimise the harm caused by cyber incidents
* leading a cross-jurisdictional training exercise to simulate how DGS and its partners would work together to respond to a high impact cyber security incident under the newly revised Whole of Victorian Government cyber emergency management and incident response plans
* developing a comprehensive training program to provide Class 2 State Controllers for Cyber Security Emergencies with the knowledge, skills and experience to effectively respond to cyber security emergencies.

DGS has improved the Victorian Government’s approach to procuring cyber goods and services by establishing four State Purchase Contracts. The streamlining of procurement for cyber goods and services has saved time and money and improved the quality of cyber services used by the public sector. Additionally, DGS is developing a Supply Chain Cyber Risk Management Framework to support the public sector better manage third party risk.

The *Administrative Guideline on the safe and responsible use of Generative AI* was issued in November 2024. The Administrative Guideline advises the VPS on the safe and responsible use of Generative AI tools and technologies for official work purposes. It also sets out minimum requirements for use, including an expectation that there is education and monitoring of Generative AI tools’ use. Additionally, Public sector organisations were provided editable Generative AI training assets to boost their awareness of its benefits and risks.

DGS is leading targeted cyber security programs in collaboration with several partner agencies to uplift and strengthen the cyber defences of selected high-risk organisations. These programs will help safeguard the critical services these organisations deliver. They also establish a repeatable framework that will enable DGS to extend similar cyber security support to the broader VPS in the future.

**Boosting cyber security skills, talent and career pathways**

DGS is providing a unique entry pathway to build high-demand skills and help create job opportunities in cyber security with a focus on women and recent graduates.

Building on the success of last year's internship program, DGS employed seven Certificate IV Cyber Security graduates in a six-month internship program where they gained hands-on experience working alongside cyber security experts. This internship program continues to help Victorians learn new skills and build the cyber and digital workforce.

DGS also worked closely with the Department of Jobs Skills Industry and Regions (DJSIR) to help champion cyber security workforce diversity.

The Women in Security program is supporting over 100 women with pathways to transition into cyber jobs and cyber leadership roles. The program provides participants with specialised training and certification, mentorship, career support, and networking opportunities.

DGS continued its work with Code Like a Girl to spotlight and address gender inequality in the sector. DGS hosted a booth at a Virtual Engineers Summit where over 200 attendees came together to build the career confidence and employability of people who identify as women, non-binary and gender diverse.

**Supporting the continued growth of Victoria’s cyber industry**

The Victorian Government continued to support the growth of the cyber industry, marketing Victoria as a place to invest.

In November 2024, we sponsored CyberCon for the third consecutive year. CyberCon Melbourne is the largest cyber security conference in the southern hemisphere, attracting over 5,600 attendees in 2024, with an estimated economic contribution of $18.3 million.

Global Victoria and the Victorian Government's Trade and Investment offices in the US are delivering a trade program providing Victorian cyber security companies with flexible market engagement support.

Additionally, Business Victoria delivered a range of tailored programs to help businesses start, grow and thrive, including ensuring they have the right cyber security settings in place. In 2024-25, more than 950 businesses participated in workshops, webinars and online learning related to cyber security and online trading.

**Building improved cyber security resilience for the community and across industries**

We continue to improve cyber awareness and understanding through the delivery of tailored programs.

Through our Service Victoria platform, DGS delivered a suite of interactive, educational digital tools that have collectively been used over 100,000 times, including a password strength tester, cyber safety health check, and two which help identify scams.

DGS supported Victoria’s most vulnerable groups to engage safely online. Partnering with local councils and Victoria Police, we delivered a series of information sessions for older Victorians on cyber safety basics and how to recognise scams.

Victoria’s multicultural communities have also been supported with in-language translation for content on vic.gov.au/stay-safe-online and campaigns, including during Cyber Security Awareness Month. Translated assets have been shared with over 70 multicultural organisations.

DGS continued to facilitate cross-government collaboration and information sharing through its communities of practice. Growing in membership each year, cyber security professionals across public sector organisations and councils were provided timely access to critical cyber updates and dedicated channels to enable more effective collaboration.

I am pleased to share this report on the actions taken to deliver the Victorian Cyber Strategy 2024-25 Mission Delivery Plan.

The 2025-26 Mission Delivery Plan sets out our continuing and new priorities for the year ahead, as we build improved cyber security resilience for government, industry, and the community.