South Australia Police submission to
Australia's Parliamentary Joint Committee on Law Enforcement
Inquiry into the capability of law enforcement to respond to cybercrime

On behalf of the South Australia Police (SAPOL) I value the invitation to make a submission to the Committee. This submission will reinforce the need for law enforcement to continue to work collaboratively with other government and non-government agencies to respond to cybercrime, the consideration for contemporary legislation and or alternate cooperation agreements and the continued need to reduce harm to the community with crime prevention messaging and the recovery of funds.

Existing law enforcement capabilities in the detection, investigation and prosecution of cybercrime, including both cyber-dependent crimes and cyber-enabled crimes.

SAPOL have adopted a tiered model for the investigation of all crime related matters, including cyber-dependent and cyber-enabled crimes. Tier 1 investigations are managed within policing districts, Tier 2 investigations are managed by specialists within Crime Service and Tier 3 investigations which impact at a state or multi-agency/jurisdictional or national scales are managed by Crime Service whether conducted within a branch or as an investigational taskforce of any construct.

Financial and Cybercrime Investigation Branch (FCIB) provides a highly specialised and professional investigation service for complex and/or organised financial, cybercrime and digital forensic services that is beyond the resource capabilities and/or expertise of other Crime Service Investigation Branches, Districts and Regions.

To develop SAPOL's capability to investigate and disrupt cybercrime, FCIB provide foundational training to all SAPOL officers to increase organisational knowledge to investigate Tier 1 cybercrimes. To increase FCIB capability members undertake training with other law enforcement agencies, government and non-government agencies.

Report Cyber is the national reporting platform managed by the Australian Cyber Security Centre. The triage process involves a desktop investigation and timely financial tracing to assist victims with the recovery of funds lost to cybercrimes, including crypto currency. Key focuses are target hardening and education to prevent re-victimisation, referral to support service and limit the financial impact on victims. FCIB commenced a pilot program in 2023 involving six investigators to triage reports received via Report Cyber and allocate them for investigation. The pilot resulted in improved service delivery for vulnerable victims, the recovery of $3.99 million through financial kill chain processes, and 110 successful website takedown requests. In May 2025, the pilot was formally established as a permanent team within FCIB.

Victims of cybercrime range from state based, transnational and international individuals as well as business entities. As perpetrators are often offshore and out of reach of Australian jurisdictions, investigation and apprehension of suspects is often frustrated, thus an increased focus is placed on victim support, crime prevention messaging and the recovery of funds for victims.

South Australia recently introduced legislative reform targeting the creation and sharing of deepfake content, strengthening law enforcement's ability to respond to cyber enabled abuse. The laws make it an offence to produce or distribute artificially generated content that is humiliating, degrading or invasive, with tougher penalties where minors are involved. The legislation specifically references artificial intelligence as a method used to generate such content, recognising its role in the rise of this emerging threat. This reform enhances investigative and prosecution capabilities by addressing a previously unregulated area of online harm and reflects a broader shift toward equipping law enforcement with tools to combat emerging forms of digital exploitation.

International, federal and jurisdictional coordination law enforcement mechanisms to investigate cybercrimes and share information related to emerging threats.

SAPOL partners with all state and territory law enforcement agencies, the Australian Federal Police and other Commonwealth agencies to respond to cybercrime threats. Since October 2023 a SAPOL member has been seconded to work in the Joint Policing Cybercrime Coordination Centre (JPC3) based in Sydney, New South Wales resulting in an increase in information sharing between SAPOL and the JPC3. SAPOL is a member of the Serious and Organised Crime Coordination Committee (SOCCC), Operation HELIOS (National Cybercrime Working Group) and the cybercrime Joint Management Group, ensuring a nationally coordinated response to cybercrime.

SAPOL utilises the Report Cyber platform to administrate, transfer and share information with national agencies. The platform has significantly increased the capability to share information, but there are limitations in the size of data sets that can be shared across this platform.

The increasing prevalence of cybercrime facilitated through foreign-owned online platforms presents significant challenges for Australian law enforcement, particularly in accessing electronic evidence stored offshore. To address this, the Australian Government has implemented the International Production Orders (IPO) framework, enabling law enforcement agencies to directly request electronic data from communications service providers in countries with which Australia has a designated agreement. The agreement allows Australian agencies to issue IPOs directly to international providers, streamlining access to evidentiary data for investigations into serious crimes, including cybercrime.

While SAPOL is not yet a direct user of the IPO framework, its integration will be considered as part of SAPOL's future capability development. Aligning with these contemporary instruments will ensure timely, lawful, and effective access to cross border digital evidence. This will significantly increase jurisdictional coordination and investigative ability, particularly in cases involving transnational digital infrastructure and emerging threats.

Coordination efforts across law enforcement, non-government and private sector organisations to respond to the conduct of cybercrimes and risks of cybercrime.

To ensure enhanced cooperation, coordination and information sharing between agencies SAPOL regularly collaborates with other LEA's and government and non-government organisations.

Report Cyber serves as a database of victim reported cybercrime and a repository for information relating to suspicious social media accounts and fraudulent bank accounts. Sharing information with banks and social media platforms through the Report Cyber platform serves several critical purposes in the fight against and disruption of cybercrime. Collaboration enables the timely identification of potential threats, leading to improved security measures by financial institutions and social media platforms. By assessing risks associated with specific accounts or profiles, banks and social media platforms can enhance their protective measures, thus creating a safer digital environment for all users. Overall, this proactive sharing of information acts as a powerful tool in preventing and deterring cybercrime, contributing to the collective effort to establish a secure online landscape.

Information sharing with the financial sector is essential to investigation, disruption and prosecution of cybercrime offences. Enhanced and continued cooperation, coordination and information sharing between the financial sector and law enforcement is required to reduce the impact of cybercrime on the community.

Emerging cybercrime threats and challenges affecting Australian entities and individuals, including the scale and scope of cybercrimes conducted in Australia or against Australians.

SAPOL continues to work in close partnership with the Australian Cyber Security Centre and the Joint Policing Cybercrime Coordination Centre (JPC3) to assess the scale and scope of cybercrime offending. Since 2020, cybercrime reports submitted via the national ReportCyber platform have shown a steady upward trajectory, peaking in 2023. A modest decline followed in 2024, and current projections suggest a further reduction by the end of 2025. South Australia has consistently accounted for approximately 7% of national cybercrime reports which is an expected proportion given the state's share of the national population. In practical terms, this equates to a 3% decrease in reports from 2023 to 2024, followed by a projected 9% decrease into 2025, representing a cumulative decline of around 12% over two years.

A notable trend emerged in the area of sextortion and Online Image Abuse offences, which experienced an escalation in the second quarter of 2022. Offence volumes during this period increased to approximately 2.5 times the levels observed prior to the spike. This elevated rate persisted through to mid-2023 before tapering off in the latter half of the year. Since early 2024, monthly reporting has stabilised at around 20 incidents per month, representing a sustained increase of approximately 30% compared to 2021 baseline levels, even after the post-spike correction.

Business Email Compromise (BEC) remains a significant threat, exploiting trust within business processes and relationships to extract sensitive information, financial assets, or goods. Offenders either compromise legitimate email accounts or impersonate trusted senders to deceive business partners, customers, or employees. While BEC was previously identified as the most rapidly escalating scam type in South Australia, particularly when measured by financial loss, recent data indicates a reversal in this trend. Reports of BEC have declined by approximately

39% between the 2022/23 and 2024/25 financial years. More significantly, the total financial losses associated with these incidents have dropped by 64%, falling from $8.5 million to $3.1 million over the same period. This suggests both a reduction in offending and improved resilience or detection within the business community.

FCIB has observed a growing trend in the use of cryptocurrency by offenders seeking to obscure their activities and evade detection. The anonymity and decentralisation of these assets present investigative challenges, requiring specialist tools and skilled personnel. Concurrently, FCIB has identified an increase in the online trade of personally identifiable information (PII), which is being used to facilitate a range of cyber-enabled crimes including ransomware attacks, investment scams, and the sale of illicit drugs on encrypted online marketplaces, including the dark web. These developments underscore the need to continue building capability to police online environments, disrupt criminal networks, and reduce community harm.

The rapid acceleration of Artificial Intelligence (AI) enabled crime represents a significant and escalating threat to law enforcement capabilities. Criminal actors are increasingly leveraging generative AI, large language models, and open-weight systems to automate, enhance, and scale illicit operations across a range of domains including financial fraud, phishing, child sexual abuse material, and romance scams. Law enforcement agencies are being outpaced by the speed, adaptability, and sophistication of these technologies, which are now functioning as effective "partners" to organised criminal groups. Compounding this challenge is the emergence of an underground economy centred on the sale of access to compromised systems and accounts. The digitisation of society has created a growing environment for cybercriminals, with cybercrime-as-a-service platforms enabling even low-skilled offenders to exploit stolen credentials, deploy ransomware, and monetise digital vulnerabilities at scale.

The public spotlight on widespread breaches of commercially held PII has likely contributed to a rise in identity theft and fraud-related reporting. These offences have increased by approximately 5.3% year-on-year, in contrast to the downward trend in cybercrime reporting. While a portion of these breaches stem from the physical theft of identity documents with the most common being driver's licences, the majority now originate from large-scale online data breaches affecting both major corporations and smaller enterprises. Offenders use stolen PII to accumulate debt in victims' names or to impersonate trusted institutions such as banks, thereby increasing the likelihood of successfully defrauding individuals. Although secondary losses from fraudulently obtained credit are difficult to quantify, the reported financial impact of identity-related offences has risen sharply, by 41% from $7.5 million in 2023/24 to $10.6 million in 2024/25.

These trends highlight both the evolving nature of cybercrime and the limitations of the current legislative framework in enabling timely and effective law enforcement responses. As cybercriminals continue to adapt, so too must the tools, capabilities, and legal mechanisms available to investigators. A forward-leaning approach that includes legislative reform, enhanced public-private collaboration, and sustained investment in digital policing capabilities will be essential to mitigate risk and protect South Australians from emerging cyber threats.

Cybercrime investigations in South Australia are often limited by the ability to lawfully access cloud-based evidence. Where a Commonwealth offence is identified, SAPOL works with Commonwealth authorities to obtain relevant data. In cases where no Commonwealth offence applies, access is restricted to matters involving child exploitation. Outside of these circumstances, SAPOL can only access cloud-based data with the consent of the account holder or entity that controls the data. This has been raised with the South Australian Attorney General's Department.

Prevention and education approaches and strategies to reduce the prevalence of victimisation through cybercrime.

FCIB is committed to providing training for members from recruit through to specialised investigation level training. The section is responsible for the development, coordination and delivery of programs and curriculum to meet cybercrime investigation training needs for the whole of SAPOL.

FCIB supports the education of businesses and members of the community around online safety, emerging trends, cyber bullying and security providing a higher level of awareness and up to date prevention measures, including target hardening and remediation processes. FCIB have developed a scams webpage on the SA Police website which educates South Australians in relation to the types of scams that are circulating, latest trends, prevention measures, reporting platforms and support services available.

To safeguard the community and business FCIB participate in national campaigns including Scam Awareness Week, National Password Day, e-smart week and Cyber Security Awareness Month through television and print media, social media and crime prevention video releases. Messaging is directed at specific demographics to support crime reduction. Further, FCIB attend community events and seminars in collaboration with other government agencies, including the SA Department of Premier and Cabinet in support of Cyber Security Awareness.

[redacted]

Linda Williams APM LEM
DEPUTY COMMISSIONER OF POLICE
Acting Commissioner of Police

1 / 9 / 2025