WESTERN AUSTRALIA POLICE FORCE

OFFICE OF DEPUTY COMMISSIONER
POLICE HEADQUARTERS
6TH FLOOR
2 ADELAIDE TERRACE, EAST PERTH
WESTERN AUSTRALIA 6004
TELEPHONE: (08) 9222 1925

Your Ref:
Our Ref: fA2804387
Inquiries: commissioner@police.wa.gov.au

Committee Secretary
Parliamentary Joint Committee on Law Enforcement
PO Box 6100
Parliament House
Canberra ACT 2600

BY EMAIL: le.committee@aph.gov.au

Dear Mr Palethorpe

INQUIRY INTO THE CAPABILITY OF LAW ENFORCEMENT TO RESPOND TO CYBERCRIME.

Thank you for your correspondence dated 6 August 2025 inviting the Western Australia Police Force to provide an updated submission to the Parliamentary Joint Committee on Law Enforcement.

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

The WA Police Force maintains a tiered capability in the detection, investigation and prosecution of cybercrime, including both cyber-dependent and cyber-enabled crimes. This capability is coordinated by the WA Police Force Financial and Cyber Crime Division (FCCD). The Agency has endorsed the WA Police Force Cyber Crime Strategy 2025 - 2028. The strategy provides a framework for the WA Police Force to increase its capability and capacity in cybercrime investigation.

This year, the WA Police Force created the Cybercrime Squad (CS) within the FCCD. The CS provides specialist advice and assistance where necessary to investigators and external partners. The FCCD has two officers seconded to the Australian Federal Police (Western Command) Cyber Operations Team. This initiative will expedite capability uplift and enhance investigator skillsets, whilst increasing overall capacity through greater collaboration and shared experience.

The division has an officer seconded to the Joint Police Cyber Coordination Centre (JPC3) in Sydney. Both secondments allow for the exchange of skills and experience in dealing with cyber-dependent and high-volume, high-value cyber-enabled crime.

The capability and responsibility of the tiers are as follows:

1. Tier 1 - Every officer has basic level of training and understanding of general offences and investigation techniques. This is generally sufficient for most low value, low complexity cyber-enabled crimes.
2. Tier 2 - Detectives are provided a fundamental level of understanding and training to manage medium level value and complexity cyber-enabled offences.
3. Tier 3 - Specialist teams investigate and prosecute high value and complex cyber--enabled crimes. These teams are capable of managing the cyber-dependent crimes.

The recruitment of staff possessing the necessary skills and the provision of specialised training presents ongoing challenges in the current competitive landscape. Similarly, the associated costs of maintaining contemporary skills, hardware, and software are compounded by the rapid advances in technology.

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

The WA Police Force partner with the Australian Federal Police (AFP) to coordinate liaison with international partners, via the JPC3 in Sydney, New South Wales.

The JPC3 provides a centralised coordination functionality to exchange data with national, state and territory law enforcement partners as well as support services such as IDCare and commercial partners, including the financial sector.

The Report Cyber portal provides the WA Police Force the ability to receive, document and transfer investigation files to other Australian jurisdictions. This platform facilitates a centralised repository for intelligence and operational metrics. The WA Police Force strongly encourages further development of the Report Cyber platform to provide data analytics, machine learning and data (pattern) matching capabilities, along with greater connectivity to partner platforms to enhance policing outcomes.

The admissibility of shared international data remains a significant challenge due to the existing Mutual Legal Assistance Treaty process which remains antiquated, slow and laborious. This process places investigations and prosecutions at risk due to the timeframes involved. Delays in identifying, preserving evidentiary items and proceeds of crime makes any subsequent capture or seizure even more unlikely the more time passes.

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

With Australian jurisdictions having separate and at times disparate laws, it makes coordinating law enforcement efforts across multiple jurisdictions difficult. Standardised or model laws are strongly recommended.

While many non-government and private sector organisations are willing to assist law enforcement, they are hesitant due to confusion regarding their ability to disclose and

share data or comply with various law enforcement instruments such as orders to produce. This is aggravated due to the limitations of reach of many state-based statutes. The model and reciprocal law recognition could assist and improve investigative capability.

The Cyber Crime Working Group is the national policing coordinating group that brings law enforcement and intelligence agencies together to provide a consolidated approach to tackle cybercrime. The operation is complimented by the JPC3. The JPC3 has demonstrated its value in this regard with recent operations in Western Australia, targeting scams involving unlawfully obtained mobile phones and cash sent through the postal service. The WA Police Force would support further expansion of the JPC3.

The Report Cyber platform provides means for agencies to share data amongst multiple jurisdictions. The controlled sharing of data with non-government and private sector organisations could assist in the prevention of cybercrimes, reducing harm to the community. An example of this would be sharing of certain information with the banking industry to identify nefarious bank accounts and bank customers. The banks could then either block or limit the activities whilst sharing the data back to law enforcement.

Government, industry and academia are a merging sector aiding in the training and education of law enforcement as well as the wider community. Cybercrime results from a failure of sufficient cyber security and or awareness. Industry and academia need to be better engaged so they in turn can do better in building cyber resilience and cyber risk awareness.

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

Australian citizens and businesses are constantly under attack on many levels in the cyber space. Businesses face a number of vectors of attack that can seriously destabilise their trading platforms and business continuity. The leading issues for business are:

- Ransomware attacks
- Phishing and social engineering
- Business email compromise
- Financial fraud and identity theft
- Cyberattacks, data breaches and data theft
- Dark web activities that provide a market for stolen data and commodities
- Private individuals face similar issues:
- Investment fraud
- Social media marketplaces
- Romance scams
- Child exploitation
- Scam calls and texts

e. The opportunities and challenges of the existing legislative framework in supporting law enforcement to investigate and act upon instances of cybercrime;

- The WA Police Force are unable to lawfully access data stored 'in the cloud' without the consent of the entity that owns or controls the account under which the data is stored. Many applications and service providers store data in the cloud (or remote servers) independent of the user's knowledge or intent. Many of these cloud and service providers are multinational with the data stored in multiple locations around the world. As the data is stored external to Western Australia, the data is effectively untouchable by the WA Police Force.
- Many organisations that possess data sought by the WA Police Force, such as banking records, are located outside of Western Australia. The current instrument for obtaining records, an 'Order to Produce' is only valid within Western Australia. Therefore, the WA Police Force rely on cooperation and the goodwill of the organisation concerned, which can be made difficult due to privacy implications.
- The freezing and seizure of fraudulently obtained funds located within banking and cryptocurrency accounts continues to hamper police and frustrate victims. The WA Police Force do not currently have legislation to compel a financial institution to suspend or return funds once identified as being stolen. Criminal confiscation legislation allows seizure of funds that are identified as being derived by criminals in the course of illicit business, but no legislation exists for recovery of scam funds.

While legislative amendments to the Western Australia statutes are sought to rectify these impediments, the challenges raised in Items (b) and (c) remain. It is strongly recommended for there are standardised or model laws.

There is an opportunity that exists for legislative amendments relating to data sharing via the Report Cyber platform. The automatic resolution of bank account holder details from bank account numbers submitted in reports made to report cyber would significantly enhance police ability to respond in a timely manner. This automated process could save time and resources of the financial sector. It should be acknowledged police will be obtaining this data via lawful means in any event as it is critical to the investigation. Further, particularly in preventing business email compromise scams, to legislate the banking sector to require full BSB, account number and account name when completing electronic transfer of funds. These details are already requested and captured; however, the account name is the one factor not checked and matched prior to transfer, which enables scammers to receive fraudulent funds.

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

The WA Police Force currently rely on the prevention outreach program of the JPC3. As a JPC3 partner, IDcare have increased their capacity to provide support to scam victims and continue to monitor the dark web for stolen data.

The WA Police Force would like to see more industry and academia engagement in the prevention and education environment.

Yours sincerely

KATE TAYLOR APM
ACTING DEPUTY COMMISSIONER

19 August 2025