WESTERN AUSTRALIA POLICE FORCE

OFFICE OF COMMISSIONER OF POLICE
POLICE HEADQUARTERS
6TH FLOOR
2 ADELAIDE TERRACE, EAST PERTH
WESTERN AUSTRALIA 6004
TELEPHONE: 131 444

Your Ref:
Our Ref: fA2823671
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

PARLIAMENTARY JOINT COMMITTEE ON LAW ENFORCEMENT - INQUIRY INTO COMBATTING CRIME AS A SERVICE

Thank you for your correspondence dated 6 August 2025 inviting the Western Australia Police Force to provide a submission to the Parliamentary Joint Committee on Law Enforcement's inquiry into Combatting Crime as a Service (the Inquiry).

For the purposes of this submission, crime as a service is taken to mean Cybercrime as a Service (CaaS), which occurs when cybercrime offenders sell their expertise in the form of tools, subscriptions or actual offending. Against the inquiry's terms of reference, the WA Police Force make the following comments regarding CaaS:

1. CaaS is not a new phenomenon, it has existed since the advent of the internet and will continue to exist as long as there is a criminal marketplace for specialist cyber skills. This marketplace is projected to grow as technology evolves.

2. CaaS skills are traditional computer science skills being applied to criminal purposes. Training and education in these skills is widely available in the education and training sector as well as the online environment, the latter including large quantities of free material. The WA Police Force submit that attempting to disrupt CaaS by targeting the training environment is unlikely to deliver substantial results, and focus should remain on community education and crime prevention.

3. It is the WA Police Force's position that there is limited benefit in distinguishing CaaS offences from non-CaaS offences. Identifying CaaS offences can be a difficult exercise, and the distinction has no meaningful effect on the investigation or management of the offence. Police target principal offenders and parties to the offence, pursuant to the

Criminal Code Act 1913 which includes CaaS entities who are applying their skills. In practical terms, any discussion about CaaS is a discussion about cybercrime.

4. Cybercrime offences, including those committed via CaaS, are investigated and prosecuted where sufficient evidence exists. Inhibitors to effective investigation include:

   a. Cumbersome international information acquisition laws and processes. Cybercrime offending is a high pace, dynamic activity where evidence is easily lost or concealed. This is a very difficult area for all governments to administer where traditional information acquisition processes, privacy and civil liability litigation combine to inhibit the timely acquisition of information by law enforcement.

      Progression is being made in this area with new legal processes such as International Production Orders, and online data seizure laws which focus on the person who accesses and controls the data rather than the geographic location where the information is actually stored.

   b. Under-reporting, which creates a low-risk and high-reward environment which unintentionally influences offenders by allowing them to use their skills on actual victims with little chance of apprehension.

      Progression is being made in this area with new reporting regimes such as the mandatory reporting laws introduced in the *Cyber Security Act 2024* and the emerging ransom-ware reporting requirements.

      The WA Police Force continue to experience two main issues with large entities:

      - Fear of brand damage and corporate embarrassment motivates entities to avoid reporting; and
      - Cybercrime events are treated exclusively as cyber-security matters. While cyber-security is an essential component of cybercrime management it has no offender management role, powers or abilities.

      Progress has been made in this area by the mandatory reporting laws already mentioned, though the majority of corporate entities remain reluctant reporters.

      The Office of Digital Government in Western Australia has transformed the Cybercrime reporting environment for state government entities. They achieved this by implementing a centralised point of control which identifies offences, then assists entities to report and liaise with police. This model has been critical for enabling the WA Police Force Cybercrime Squad to conduct rapid, effective, offender management action in Cybercrime offences against state government entities.

      This centralised consolidation model is also mitigating one of the largest challenges facing small to medium sized entities, namely insufficient resources to implement effective cyber-security.

   c. The large number of cyber related reporting systems in Australia conceals the scope, impact and patterns of offending by fragmenting the information across numerous isolated data silos.

d. There is very limited analysis of cybercrime offending at a national level which focuses on the high volume, low value offending which constitutes the majority of cybercrime. This is a consequence of the traditional roles of Australian police agencies, where state and territory police manage high volume crime and federal entities manage high severity, national crime.

   For the first time, Cybercrime has made high volume crime a routine national occurrence. It is fair to say that our federal entities may not be unfamiliar with, nor resourced for this challenge as it is not typically their working environment.

   Adjustment of the national Cybercrime policing model is highly recommended to ensure Cybercrime is addressed, and the structure of our layered national policing model maintained. This could be achieved by implementing state/territory style policing activity in the national environment which:

   - Triages work to the appropriate agencies, which includes other Cybercrime stakeholders;
   - Analyses of offending data to identify and prioritise offenders based on the harm they cause; and
   - Provides strategic information to decision makers as detailed in the following point.

   Progress is being made in this area as detailed in point (e) below.

e. The absence of a consolidated cybercrime statistics at the state and national levels impacts the ability of police agencies and governments to understand, resource and direct Cybercrime management initiatives.

   Progress is being made on points (e) and (f) through the creation of the Joint Cybercrime Coordination Centre in Sydney. While this centre is progressing well further refinement is required, this has been identified and is under consideration by the Australian Federal Police executive.

f. The National Cybercrime Reporting System requires further enhancement to meet policing needs. A critical issue remains the absence of information analysis and statistical reporting functions. Progress is being made in the area through the planned development of a new system.

   The WA Police Force believe this project would benefit from a re-statement of the original design objectives which were made by the 2010 Parliamentary Review into Internet Crime. Recommendation 4 of that report related to the national reporting system and could form the basis of a statement of design intent for the new system.

5. The current combination of Commonwealth and Western Australian laws are sufficient to address Cybercrime offending.

6. CaaS creators and suppliers are also investigated and prosecuted where sufficient evidence exists. The investigation of CaaS creators or suppliers who are directly involved in offending is an automatic occurrence as they are a party to the offence and deemed an offender.

The investigation of CaaS creators or suppliers are not directly involved in offending, such as the creators of tools, is a resource and time intensive activity with difficult evidentiary requirements.

7. The WA Police Force are observing a steady increase in sophisticated and organised Cybercrime offending with increasing elements of CaaS. The CaaS concept, being the use of technologically skilled individuals to enable cybercrime offending, continues to evolve in line with this.

   An example includes the victim management systems being implemented in scam centres, which enable the scam centre workforce to interact effectively with multiple victims concurrently, understanding maintaining the scams all of which are progressing at different speeds with different nuances. The ongoing professionalisation of cybercrime offenders presents a challenge for police and governments, particularly in the area of skills parity.

   Improved information reporting as mentioned at point 4(e), and increased resourcing in line with the recognised uptick in cybercrime offending should assist in this area.

Should the Committee have any questions relating to this submission, please contact [redacted]

Yours sincerely

[redacted]

COL BLANCH APM
COMMISSIONER OF POLICE

30 September 2025