PARLIAMENTARY JOINT COMMITTEE ON LAW ENFORCEMENT

INQUIRY INTO THE CAPABILITY OF LAW ENFORCEMENT TO RESPOND TO CYBERCRIME

Australian Federal Police

Written questions on notice

Senator Polley asked the following questions on Thursday 14 November 2024:

1. Regarding ReportCyber reports:
    a. Can you please provide more information about how the current triage and analysis system works?
    b. At the hearing on 22 October 2024, the AFP suggested there may be scope for improvements to triage (*Proof Committee Hansard*, p. 18). Could you please provide more information about any improvements that are envisaged? Is any work planned or underway to:
        i. better manage the volume of reports, and
        ii. provide further support for state and territory police agencies which may face resourcing challenges?
2. Could you provide further information on the operation and intended outcomes of Project Unity? How will it improve data analysis and enhance coordination across jurisdictions? How many staff are working on Project Unity and from which jurisdictions?
3. The Cyber Security Cooperative Research Centre advised that the JPC3 recently held Australia's first cybercrime prevention forum (*Proof Committee Hansard*, 16 October 2024, p. 8). Could you please provide some details about the forum? Who participated and what did it achieve?
4. The committee has heard positive evidence about the JPC3, including that it could be rolled out in other locations (e.g. Cyber Security Cooperative Research Centre, *Proof Committee Hansard*, 16 October 2024, p. 7) and built on the model of the Australian Centre to Counter Child Exploitation (e.g. CyberCX, *Submission* 27, p. 9). Is any work underway to expand or continue to improve the JPC3? Are there aspects of the ACCCE that could be incorporated into the JPC3?
5. Evidence to the committee suggests there is a range of education and public awareness work underway (See *Proof Committee Hansard*, 16 and 22 October 2024). Is there an overarching strategy in relation to public awareness to ensure educational activities are coordinated between agencies and consistent? How is the AFP ensuring its messaging is effective?

6. At the hearing on 22 October 2024 the AFP mentioned funding and work underway on a training curriculum for the AFP, states and territories (*Proof Committee Hansard*, p. 18). Can you please provide more detail about this curriculum, including the level of funding, the proposed timeline for implementation, and who will receive the training?
7. The committee has heard there may be a need to address workplace practices that disincentivise specialisation in cybercrime investigations (e.g. Dr Cassandra Cross, *Submission* 14, p. 12). Can you please elaborate on whether this is an issue and how the AFP ensures that cybercrime specialisation is an attractive option?
8. The AFP previously advised that it would pilot re_B00tCMP in March 2024 (*Submission* 22, p. 18) and the Cyber Security Cooperative Research Centre noted the pilot was successful (*Proof Committee Hansard*, 16 October 2024, p. 8). Can you please provide some information about the program, the evaluation of the pilot, and future intervention programs?
9. The Cyber Security Cooperative Research Centre mentioned work done by ANZPAA in relation to protocols for dealing with cybercrime (*Proof Committee Hansard*, 16 October 2024, p. 8). Can you provide the committee with this information?
10. The Cyber Security Cooperative Research Centre raised an issue regarding the AFP's ability to use artificial intelligence and data retention laws (*Proof Committee Hansard*, 16 October 2024, p. 10). Can you please respond to this concern: is it an issue from the AFP's perspective? Is any work underway in relation to the issue?
11. Noting the AFP's advice that existing Commonwealth legislation is adequate for efforts to counter cybercrime offshore (*Proof Committee Hansard*, 22 October 2024, p. 19), does the AFP have a view about the issues raised by CyberCX regarding section 43C of the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021*? (see *Proof Committee Hansard*, 22 October 2024, pp. 2–3 and *Submission* 27).

The response to the senator's question is as follows:

1. (a) Responsibility for the overall technical delivery and management of ReportCyber rests with the Australian Signals Directorate (ASD). Information on how ReportCyber's internal triage and analysis system operates should be addressed to ASD.

   (b) The improvements noted are in reference to Project Unity.

   (i) This project seeks to automate and enhance ReportCyber data and processes and make connections across reports of cybercrime. Law enforcement will be able to quickly view and search intuitive and easy-to-read visual representations of cybercriminal or victim connections and other related information such as names, key words, street, email and IP addresses, and bank account details.

   (ii) Allocation of state and territory resources are a matter for respective agencies. Project Unity aims to reduce the burden on individual agencies by providing a more nationally consistent and collective insights to ReportCyber referrals.

2. Project Unity is an ongoing project that seeks to enhance data within ReportCyber, enabling a swift, nationally informed and coordinated response to cybercrime through:

    a. enhanced visibility of work on hand and the ability to triage, analyse and process cyber reports more quickly.

    b. Intelligence capability enhancements providing visual representation of connections and providing a national picture.

    c. Improved information sharing and engagement between jurisdictions.

    The AFP is leading the coordination of this Project which contains seven members. The Project has established a Stakeholders and Business Working Group, with representatives from all state and territory police jurisdictions, the JPC3, Defence and ASD / Australian Cyber Security Centre.

3. In August 2024, the JPC3 Prevention hosted the first National Cybercrime Prevention Forum in Australia, bringing together law enforcement, government, industry and academia from across the country to share knowledge, network and identify opportunities for collaboration. The AFP partnered with the Dutch National Police on this event:

    - Day 1 – in partnership with the Dutch National Police, focused on innovative strategies aimed at preventing potential offenders from entering a life of cybercrime.

    - Day 2 - 'whole-of-society' approach to victim prevention and explored collaborative strategies to build Australia's cyber resilience.

    The Forum allowed for collaboration and knowledge sharing with key areas of prevention highlighted, including the need for education, disruption and victim support.

    Following the success of the Forum and feedback from attendees, the JPC3 intends to host this forum annually in August.

4. The JPC3 was established in March 2022 to support the National Plan to Combat Cybercrime, and the current funding envelope for the JPC3 is fully allocated. The JPC3 model recognises the primacy of the states and territories in responding to many cybercrimes, by providing national coordination to target high volume and high harm cybercriminal syndicates.

    Both the JPC3 and ACCCE are established on similar principles of collaborative centres to coordinate and drive effort and harness shared capabilities. The JPC3 is an effective and nationally supported model for bridging the gap between the AFP focus on transnational organised cybercriminal syndicates and the volume reporting experienced by states and territories. The AFP has dedicated cybercrime teams located in Brisbane, Perth, Melbourne and Sydney with each team having close partnerships with their state or territory counterparts.

The JPC3 and ACCCE are both AFP-led and work closely and collaboratively together on common issues, complementing their distinct areas of focus.

The AFP will continue to look at opportunities to enhance the work and reach of the JPC3 across law enforcement, regulatory agencies and the private sector.

5. Education and public awareness priorities for law enforcement are coordinated nationally through the JPC3 Prevention Team-led National Cybercrime Prevention Network. This Network was established in May 2023, with representatives from law enforcement, government and industry. Through this Network, the JPC3 Prevention Strategy has been drafted and identified three core pillars for the approach: Protect, Prevent and Partner.

   The JPC3 Prevention Strategy ensures messaging and activities are effective through formal evaluation of education activities and projects, evaluation of social media reach, tracking of engagements and ongoing alignment of prevention strategies with operational initiatives. This Strategy provides a focused approach but also flexibility to align with operational priorities as they arise, including opportunities to partner law enforcement messaging with industry and agencies like ASD and the National Anti-Scam Centre.

6. The AFP has delivered national training needs analysis and is now progressing the design and delivery of the National Training Curriculum Project. Funding for this has been provided under the National Cybercrime Capability Fund, with $1.9m in current funding.

   The curriculum produced by this activity will consider training currently available for cybercrime investigators and will either supplement or replace this training. The project timelines for this require a curriculum to be drafted by June 2025, followed by 12 months of national delivery testing, adjustment and refinement. This training is intended to be provided to Australian law enforcement agencies.

7. Within the AFP we have implemented multidisciplinary teams which provides a retention of specialised technical skillsets and allowing for occasional, carefully considered rotation of investigative and intelligence skillsets.

   This allows technical experts to continue specialised concentration but ensures that our investigative and intelligence officers bring diverse operational experience and in turn, cyber experienced investigators are able to expand and share their knowledge and skills in other crime types. This multi-disciplinary approach ensures that cybercrime remains an attractive and viable option for subject matter experts, general police investigators, intelligence officers and a variety of support staff roles.

8. The 're_B00TCMP' initiative is a one-day program for 12 to 17-year-old students who are skilled in IT and tend to push the online/technology boundaries. It introduces students to career opportunities in cyber security and law enforcement and teaches them about legal online parameters. A parallel 'parent and teacher session' gives adults the tools to understand and foster the skills of the students. This adapts and builds on tried and tested practices from

programs in the Netherlands (re_B00TCMP) and United Kingdom (Cyber Choices) to effectively address cyber-related challenges among talented young individuals in Australia.

The re_B00TCMP Australia pilot program was held in Sydney on 5 March 2024, with positive responses from attendees, parents and stakeholders. The need for ongoing programs of this nature has been reiterated through a number of engagements and it has been identified as a law enforcement priority for cybercrime prevention. Planning is underway for a further program to run in Queensland, with interest in national rollout.

9. ANZPAA first developed a protocol for cybercrime in 2011 and have reviewed these arrangements on a regular basis, with the latest review finalised in March 2024.

   The protocol details an outcomes-focussed approach and guidance for law enforcement agencies responding to and managing cybercrime in Australia and New Zealand. It aims to enhance outcomes for victims through the disruption of cybercrime and provide cross-jurisdictional consistency and clarity in the response to and management of cybercrime.

   It aims to work in conjunction, but does not supersede, other instruments that relate to specific aspects of cybercrime such as online child exploitation. Any further queries in relation to this protocol should be directed to ANZPAA.

10. The AFP are committed to upholding ethical and responsible practices in the utilisation of artificial intelligence (AI) through its AI Principles, which will guide the AFP as it adopts, implements and operationalises AI systems. The AFP prioritises the integrity and security of data, adhering to strict data retention laws under the *Telecommunications (Intercept and Access) Act 1979* (Cth) and *Surveillance Devices Act 2004* (Cth), as well as compliance with the *Privacy Act 1988* (Cth), and other policies to protect sensitive information. The AFP is participating in whole-of-government work to develop policies and procedures on the responsible use of AI in Government, led by Department of Industry Science and Resources (DISR) and the AI in Government Taskforce, within the Digital Transformation Agency (DTA). Any reforms to relevant legislation are a matter for government.

11. The AFP notes the comments by CyberX.

    The Attorney-General's Department is currently conducting a review of Australia's electronic surveillance framework, and the Independent National Security Legislation Monitor is conducting reviews into the operation, effectiveness and implications of the *Surveillance Devices Act 2004* (Cth) and the powers of law enforcement introduced by the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* (Cth). This legislation has significantly assisted the AFP to combat transnational, serious and organised crime including cybercrime.

    Any changes to this legislation are a matter for government and such questions should be directed to AGD.