Inquiry into the capability of law enforcement to respond to cybercrime
Response to written questions on notice from the Australian Institute of Criminology

1. **At the public hearing on 16 October 2024 (*Proof Committee Hansard*, p. 2), the AIC said survey data suggest there have been improvements in cybercrime victims' satisfaction with law enforcement's response to their matter. However, only about five per cent of cases have a positive resolution. What do you believe is contributing to increased satisfaction with law enforcement?**

Since the introduction of the ReportCyber platform—which replaced the Australian Cybercrime Online Reporting Network (ACORN)—the mechanism through which victims can report cybercrime has been improved. Steps have also been taken to enhance information sharing from these reports between and within law enforcement agencies and the capability of police to respond to cybercrime reports. Although the results were not directly comparable, there appears to have been an increase in the proportion of victims who said police had indicated some action had or would be taken in response to their report. Further, the evaluation of the ACORN also showed a strong relationship between satisfaction with the process of reporting and satisfaction with the outcome (Morgan et al 2016). The fact that the platform has been improved has likely improved the user experience and, in-turn, their satisfaction with the outcome, even if the outcome of their report was the same.

Further, the evaluation of ACORN in 2016 (Morgan et al 2016) found that over three quarters of all victims who submitted a report to the ACORN felt the outcome did not meet their expectation, and this was associated with lower levels of victim satisfaction. While the ACORN website did include advice that many cybercrime reports are unlikely to be investigated, it seems that victims nevertheless had unrealistic expectations about the outcomes of their reports. The new ReportCyber platform more clearly includes advice that it is extremely unlikely that money will be recovered and victims should contact their financial institutions immediately, and that victims may be contacted by police if additional information is required, but not all reports will be investigated. Greater expectation management may have led to some improvements in the reporting experiences of victims.

There has also been a significant enhancement in law enforcement's cybercrime capability. This includes the Joint Policing Cybercrime Coordination Centre (JPC3), launched in 2022, which brings together all Australian policing jurisdictions to enhance intelligence sharing, coordinate joint task forces, and improve capabilities in responding to cybercrime. This is in additional to national task forces, and the investment by individual agencies in their own cybercrime capabilities. In partnership with law enforcement and the private sector, policing agencies have also continued to build awareness among victims of cybercrime about how to access resources on recovery and how to report incidents.

Together, these changes may have help to contribute to improved satisfaction among victims. Further evaluation of the impact of policing responses to cybercrime victims is required.

2. **At the public hearing on 16 October 2024 (*Proof Committee Hansard*, pp. 2–3), the AIC said it is working on a harm index relating to cybercrime that law enforcement would be able to use. Could you please tell the committee more about the harm index and an approximate timeframe for it to be available?**

The AIC recently developed a cybercrime harm index, which can capture the nature and extent of harms experienced by victims of different types of cybercrime. Crime harm indexes have been developed as an alternative to relying on offence frequencies and to better represent the concentration of crime-related harm among offenders, victims or places. This can assist law enforcement with prioritising crimes which are most harmful, as well as measure success or failure of different strategies and policies aimed at reducing crime harm.

The AIC adopted a novel approach that draws on victim self-report data collected through the Australian Cybercrime Survey. The index provides a measure of the relative severity of 17 common types of cybercrime, with stalking and harassment and remote access scams found to be the most harmful. Harm scores were based on a 34-item measure of cybercrime harm encompassing practical, health, social, financial and legal

impacts, according to victim reports of the prevalence and severity of each harm. We used these harm scores to measure concentration among cybercrime victims. Overall, just 10.9 percent of victims accounted for 57.7 percent of the harm to all victims who completed the survey. This research found that repeat victims who experienced multiple types of cybercrime are disproportionately impacted and should be prioritised for intervention.

A Trends and Issues paper is currently being prepared for publication. We anticipate that the harm index will be publicly released in the first half of 2025.

3. **At the public hearing on 16 October 2024 (*Proof Committee Hansard*, pp. 2–3), the AIC said its working with the Australian Federal Police and eSafety on developing awareness campaigns with different messages. Could you please provide more detail on the testing underway, as well as any strategy that supports this work? How do you ensure coordination with other agencies, in terms of both messaging and timing of campaign activities?**

The AIC recently trialled a targeted cybercrime awareness campaign in collaboration with the JPC3 of the Australian Federal Police and the eSafety Commissioner. An experimental design was used to test whether the deployment of targeted prevention messages has any impact on participant experiences of online abuse and harassment and profit-motivated cybercrime victimisation, as well as awareness of online safety, use of higher risk or protective online behaviours, repeat cybercrime victimisation and help-seeking behaviour. A subsample of 3,500 respondents were recruited from the 2023 Australian Cybercrime Survey and were randomly allocated to one of three groups: An online abuse and harassment intervention group (1,250 participants) who received monthly prevention messages from eSafety for six months; a profit-motivated cybercrime intervention group (1,250 participants) who received monthly prevention messages from the JPC3 for six months; and a control group (1,000 participants) who did not receive any messages. They were then surveyed again as part of the 2024 Australian Cybercrime Survey to measure changes across time. The experimental design means we can be confident that any changes in victimisation or online safety observed were the result of the prevention messages.

The intervention was a targeted campaign where survey participants were recruited through the online survey, consented to be involved and were sent cybercrime advice and information directly to their email accounts. The content and timing of each message was coordinated between AIC, AFP and eSafety during fortnightly meetings. The intervention commenced in October and concluded in March 2024. The AIC has yet to analyse the results of the trial and plans to produce a report on the outcomes of the research in 2025.

References

Morgan et al 2016. Evaluation of the Australian Cybercrime Online Reporting Network. Australian Institute of Criminology: Canberra. https://www.aic.gov.au/sites/default/files/2020-06/acorn_evaluation_report_.pdf