A private hearing under section 22 of the *Independent National Security Legislation Monitor* *Act 2010* (INSLM Act) with the Australian Criminal Intelligence Commission (ACIC) took place at 3-5 National Circuit, Barton ACT 2600 on Tuesday 11 March 2025.

The 6 witnesses from the ACIC were:

* A/g Chief Executive Officer
* Chief Counsel
* National Manager, Collection Operations
* Director, Encrypted Criminal Communications
* Assistant Director, Encrypted Criminal Communications
* Senior Lawyer, Law Reform

There was also one observer from the ACIC.

In addition to the Independent National Security Legislation Monitor (the Monitor), one staff member from the Independent National Security Legislation Monitor (INSLM) Office participated.

The purpose of this hearing was to enable the ACIC to provide *operationally sensitive information* in responses to questions on notice taken at their appearance on 20 February 2025 at the public hearing for the INSLM review of the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* (Cth) (SLAID Act).

## Summary

#### Opening remarks

* The Monitor opened the hearing and thanked representatives from the ACIC for their attendance.
* The Monitor noted that the purpose of the hearing was to enable the ACIC to provide responses to questions on notice that would involve operationally sensitive information.

#### Use of Network Activity Warrants

* The Monitor noted that the ACIC had provided evidence at the public hearing that network activity warrants (NAWs) had been sought for offences lower than five years.
  + The ACIC clarified that no NAWs had *solely* been sought for offences lower than five years. Some NAWs which were for more serious offences (over 5 years) have also listed at least one three-year offence.
* The Monitor asked the ACIC to expand on why (if the threshold for relevant offence was raised above three years) it would not be possible to collect intelligence on lower level offences incidentally when the groups ACIC is actually focused on are serious organised crime groups that are involved in or are facilitating higher offence crimes.
  + The Monitor noted that there would not appear to be anything in the enabling legislation, the *Surveillance Devices Act 2004* (Cth), to prevent the ACIC from using incidentally obtained information obtained under a NAW in relation to lower level offences that were not the subject of the warrant, provided that the warrant had genuinely been sought for (higher) relevant offences.
* The ACIC provided hypothetical examples based on observed behaviour of serious and organised crime groups of where the ACIC, in the exploratory stages of intelligence gathering, might become aware of activities being undertaken that are likely to be used to support the commission of more serious offences.
  + That early activity may not be unlawful or, if it is unlawful, may constitute an offence punishable by less than three years imprisonment or may be punishable by an offence of three years imprisonment.[[1]](#footnote-2)
* The ACIC said that, in the hypothetical example, if the preliminary activities constituted an offence punishable by three years’ imprisonment they would currently be able to obtain a NAW, even if they had no intelligence, at that time, linking the activity to a more serious crime. In such a situation the intelligence gathered by ACIC may enable them to have greater visibility of potentially more serious criminal behaviour that could be linked to serious organised crime.
  + However, if the threshold was increased to 5 years, the ACIC was concerned it might not be possible to obtain a NAW to collect intelligence in this type of scenario unless they had sufficient information about the particular “kinds” of serious offences that were being facilitated by these activities in order to meet the requirements for a NAW.
* It was also noted by the ACIC that they take a conservative/cautious approach when seeking a NAW, including being able to demonstrate a strong link to the relevant kinds of serious offences.

#### Use of Account Takeover Warrants as a covert power

* The Monitor noted that the Australian Federal Police (AFP) provided examples in the public hearing of their use of account takeover warrants (ATWs) in conjunction with overt search warrants. This could be compared to the ACIC, whose evidence in the public hearing and in their submission indicated that they proposed to use ATWs in a covert manner.
* The ACIC provided some examples of where they considered that they would be able to takeover an account using an ATW covertly.
  + In one hypothetical scenario the ACIC described a specific situation where using a combination of their existing powers plus an ATW they could takeover and then covertly operate an account in order to gather evidence.
    - It was acknowledged that covert operation of an account in this situation was likely to be for a short period of time as otherwise the owner of the account may discover that their account had been taken over. However, the ACIC indicated that even a short period of operating certain types of accounts was likely to be of value.
  + In another hypothetical scenario the ACIC described a situation where it would be possible to covertly operate an account for a short period of time in circumstances where other intelligence indicates the owner the account was unlikely to discover that their account had been taken over.
  + In another hypothetical example the ACIC described a situation where they could takeover an account briefly and operate it to allow later evidence collection, under other powers, more effective.
* The ACIC also gave a hypothetical example of working with a service provider, such as a financial services provider, where they believed that the use of an ATW would allow the ACIC to obtain evidence that could not be gathered using a search warrant.
* Some of the examples provided by the ACIC were more akin to intelligence gathering than strictly evidence gathering, but the Monitor acknowledged that this distinction was not always clear and at least some of the hypothetical scenarios were reasonably likely to result in admissible evidence.
* The Monitor noted that ATWs may have an incidental disruptive *effect* (for example a person who discovered their account has been taken over may cease engaging in some criminal activity) but that disruption was not the purpose of these warrants.

#### Ability to use information obtained under NAWs

* The Monitor noted that there was some uncertainty from the ACIC’s evidence in the public hearing regarding the extent to which they currently collected information under a NAW through the use of telecommunications interception (TI) and/or surveillance devices when using those capabilities for the purposes of executing the warrant.
* The ACIC outlined how TI and surveillance devices capabilities were used for the purposes of doing things specified in a NAW and the type of information that was collected using those capabilities. While that collection may be quite extensive in some situations, the ACIC emphasised that it significantly assisted them in being able to covertly execute the warrant at the right time and in relation to the right computer(s).
  + The IGIS is the body responsible for oversight of NAW use by ACIC including in relation to TI and SD undertaken to enable the NAW to be executed.
* The ACIC were primarily concerned that if they incidentally obtain information about criminal activities from TI/SD when executing an NAW they cannot use that information for any intelligence purposes, including in intelligence reports or to apply for other warrants.
  + The ACIC described internal safeguards that were applied in relation to the information collected using TI/SD capabilities including that monitoring of TI/SD is undertaken by a separate team so that only information that it is lawful to use in order to execute the NAW is passed to the ACIC officers working on the operation.
* There was some discussion about comments in the AGD submission and evidence about the policy reasons for TI/SD access having a higher threshold than NAWs and concern about an intelligence warrant with a low threshold having an effect like a ‘general warrant’.
* The Monitor noted that the legislation presently allows TI and SD material obtained to execute a NAW to be used or communicated in situations where it is necessary to help prevent or reduce the risk of serious violence to a person or substantial damage to property as well as to ASIO, ASIS, ASD and AGO.[[2]](#footnote-3) The ACIC gave examples of reaching this threshold and communicating material but was also able to provide examples of serious offending where the threshold was not reached.
  + There was brief discussion as to whether there are any other categories that are similar to those serious threats to safety/property in the existing exceptions that would justify departure from the current policy limits embodies in the legislation.

#### Necessity of ACIC having DDWs

* The ACIC outlined hypothetical scenario where, with the appropriate skills and technology, they may be able to use a data disruption warrant in the future.
* The Monitor asked why it would not be possible to work in collaboration with the AFP to obtain a DDW in such a scenario.
  + The ACIC noted that the AFP had a number of competing priorities and that there are differences in technical capabilities between the two agencies.
* The ACIC noted that some of the other powers they have access to, particularly compulsory questioning and proceeds of crime, often have a disruptive effect.
  + The Monitor noted that there is a significant difference between an action lawfully undertaken for a different purpose having a disruptive effect and a power to do something that is otherwise unlawful (disrupt data) only for the purpose of disruption. The Monitor also noted that powers such as the ACIC questioning power and proceeds of crime had detailed oversight mechanisms including the role of independent examiners and judicial scrutiny.

1. The lesser offences and the otherwise lawful activity which may indicate a link to organised crime have not been included in this published record as they indicate the type of preliminary activity the ACIC is or may be investigating. The Monitor was satisfied that for each of the examples given by the ACIC it was reasonable to expect that investigating those types of activities was linked to investigating relevant serious (5 year plus) organised criminal activity. [↑](#footnote-ref-2)
2. There are some differences between when SD information (see s45B of the SD Act) and TI information (see s63AE of the TIA Act) can be disclosed. For example, for SD information the person must believe on reasonable grounds that a disclosure is *necessary* to help prevent or reduce the risk of serious violence to a person while for TI the threshold is that the information must ‘relate or appear to relate’ to activities that present a significant risk to a perron’s safety. SD can be communicated to ASIO and the IS agencies for any of their functions, while it is more limited for the TI Act, though that Act includes additional sanctions reacted purposes for which information can be disclosed. These differences were not discussed in the hearing but are noted in this record for completeness. [↑](#footnote-ref-3)