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 Monday, 29 July 2024.

There were 10 witnesses from the ACIC that worked in the operational, legal, strategic policy and assurance areas within ACIC. The 10 witnesses were:

* A/g Executive Director, Covert Collections and Insights
* National Manager, Legal Services
* Assistant Director, Encrypted Criminal Communications
* Senior Technical Analyst, Encrypted Criminal Communications
* Assistant Director, Encrypted Criminal Communications
* Senior Intelligence Analyst, Encrypted Criminal Communications
* Principal Adviser, Integrity, Security and Assurance
* A/g Director, Integrity, Security and Assurance
* A/g Director, Strategic Policy
* Senior Lawyer and ACIC secondee to the Electronic Surveillance Reform Task Force

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

The purpose of this hearing was to:

* obtain initial information about the ACIC’s use of warrants established under the *Surveillance Legislative Amendment (Identify and Disrupt) Act 2021* (SLAID Act) including data disruption, network activity and account takeover warrants (collectively referred to as SLAID warrants), and
* ask questions about network activity warrants (NAWs) issued to the ACIC that were reviewed by the INSLM staff prior to the hearing.

## Summary

#### Opening remarks

* The Monitor opened the hearing and thanked representatives from the ACIC for their attendance and provided an outline of the review.
* The Monitor noted that the strict secrecy laws that apply to SLAID warrants made it necessary to exercise statutory powers under the INSLM Act to have a hearing in order to enable the ACIC to share all relevant information. It was emphasised that the calling of the hearing did not reflect any lack of cooperation from the ACIC.
* The Monitor said the primary purpose of the hearing was to understand how the SLAID warrants were working in practice.

#### Usage of warrants and effectiveness

* The Monitor asked the ACIC a number of questions related to the usage of the warrants and their effectiveness.
* The ACIC provided a summary on how the NAWs operate. In their original submission to the PJCIS on the anticipated use of NAWs, ACIC said these warrants would be used to gather information on criminals using dedicated encrypted communication devices (DECDs) and platforms. [[1]](#footnote-2) These were to be targeted by the ACIC because they are almost exclusively used by serious organised crime (SOC) groups in order to try to obfuscate criminal activity and identities. ACIC’s use of NAWs has been to target serious and organised crime, which is consistent with the positions put forward in the submissions.
* The ACIC said that NAWs were beneficial in understanding criminal networks, and targeting a network, providing the ACIC with an alternative tool to combat cyber-enabled crime, particularly where encryption presented challenges to other traditional investigative and disruption actions and electronic surveillance techniques.
* ACIC’s use of NAWs is for criminal intelligence collection. ACIC noted that they may use NAWs in conjunction with industry assistance powers and other collection tools.
* Overall, the ACIC indicated that NAWs have enhanced awareness of the environment that SOC networks operate within and the people they interact with. The ACIC said that information obtained from NAWs had also informed other criminal intelligence activities and had formed the basis for criminal intelligence reports.
* Annual reporting[[2]](#footnote-3)and statistics provided by the ACIC for the financial year 2023-24 indicated that only a small number of NAWs had been sought and that most of these had been extended multiple times.
  + The Monitor raised the appropriateness of the 90-day duration period of a NAW in the context of this pattern of multiple renewals. The ACIC noted there were challenges with the 90-day timeframe given that most of their operations were complex and long-term intelligence operations. The ACIC may make a submission on this issue.
* The Monitor noted that annual reporting[[3]](#footnote-4) indicated the ACIC had not used ATWs and DDWs and asked whether the ACIC could foresee a likely scenario where these warrants would be used by the ACIC – and not in partnership with the Australian Federal Police (AFP).
  + The ACIC highlighted the distinction between the criminal intelligence role of the ACIC and the traditional role of police agencies in evidence gathering for prosecutorial purposes. The ACIC emphasised that it was important that the SLAID warrants be aligned to its current and future criminal intelligence activities.
  + ACIC will give this issue further consideration and include a response in its formal submission to their review.

#### Assistance from other agencies

* The Monitor noted the Revised Explanatory Memorandum to the SLAID Act pointed to potential assistance from the Australian Signals Directorate (ASD) in the execution of SLAID warrants. The ACIC said that it had executed warrants issued since the enactment of the SLAID Act without ASD assistance.

#### Privacy implications

* The Monitor asked the ACIC to outline the process by which information relevant to a criminal offence is distinguished from third party information that could be accessed through NAWs. The ACIC explained that it is only interested in criminal activity and undertaking target collection as effectively as possible to obtain the most relevant data from target computers. All devices targeted by the ACIC were used by individuals the agency could demonstrate were members of the network of criminally linked individuals described in their NAWs. The Monitor noted that this may be an area that is further explored in the review.

#### Life cycle of data

* The Monitor asked about the nature of information sharing in connection with the SLAID warrants. The ACIC explained that information has only been passed on in the form of an intelligence product (not as raw data) through reporting to the AFP, other Commonwealth partners, intelligence agencies and foreign partners. This information sharing is done in accordance with the *Australian Crime Commission Act 2002* (ACC Act), as well as the provisions in the SD Act.
* The Monitor noted that while the disclosure provisions in the SLAID Act were robust, they did not appear to cover secondary use and disclosure by agencies that receive the information. The ACIC highlighted that this would likely be covered under the caveats that are included in the particular products where recipients must seek approval for any further use of information by the delegate who approved the initial disclosure. Any disclosure of protected network activity warrant information must be in accordance with the ACC Act, SD Act and TIA Act.

#### Location of data

* The ACIC was asked about how it knows whether data or devices are located inside Australia.
* The ACIC noted that in most cases data is known to be located in Australia by virtue of the type of targeting used by the agency via its NAWs, however in some cases the use of virtual private networks and end-to-end encryption has made it challenging to identify the location of data. The ACIC uses a combination of techniques to determine the location of data and devices. They generally have a high level of confidence that the data and devices that the ACIC is focused on are inside Australia.

#### Issuing Authority

* The Monitor noted his interest in understanding the process by which SLAID warrants are issued. There was also discussion about the fact that there is a limited pool of issuing authorities available to issue warrants in the ACT where the ACIC headquarters are located. The Monitor flagged this as a topic for further consideration in the review.
* The ACIC noted that as a matter of policy, applications for a NAW may only be made by an SES band 3 or the CEO.

1. See Australian Criminal Intelligence Commission, Submission 23 to the Parliament Joint Committee of Intelligence and Security, *Review of the Surveillance Legislation Amendment (Identify and Disruption) Bill 2020*, 2. [↑](#footnote-ref-2)
2. See Attorney-General’s Department*, Surveillance Devices Act 2004 Annual Report 2021-22* (*‘SD Act Annual Report 2021-22*’), 30 and Attorney-General’s Department*, Surveillance Devices Act 2004 Annual Report 2022-23 22* (*‘SD Act Annual Report 2022-23*’), 31. [↑](#footnote-ref-3)
3. See Attorney-General’s Department, SD Act Annual Report 2021-22 (n 1) 26; Attorney-General’s Department, SD Act Annual Report 2021-22 (n 1) 27; Australian Criminal Intelligence Commission, *Crimes Act 1914 - Account Takeover Warrant Annual Report to Minister for the period 4 September 2021 to 30 June 2022* (Annual Report, 7 March 2023) 1 < [Tabled documents | Document 1069 (aph.gov.au)](https://www.aph.gov.au/Parliamentary_Business/Tabled_Documents/1069)>; Australian Criminal Intelligence Commission, *Account Takeover Warrant Annual Report to Minister [1 July 2022 to 30 June 2023]* (Annual Report, 31 August 2023) 1 <[Tabled documents | Document 3167 (aph.gov.au)](https://www.aph.gov.au/Parliamentary_Business/Tabled_Documents/3167)>. [↑](#footnote-ref-4)