Review of the Surveillance Legislation Amendment (Identify and Disrupt) Act 2021

Submission to the

Independent National Security Legislation Monitor

18 December 2024

Table of Contents

Table of Contents 2
2. Introduction 3
3. Background 3
About the Inspector-General 3
4. Surveillance Legislation Amendment (Identify and Disrupt) Act 2021 3
Jurisdiction split between oversight bodies 4
Powers and functions to undertake oversight 5
Transparency and public reporting 5

Introduction

1. The Inspector-General of Intelligence and Security (IGIS) welcomes the opportunity to make this submission to the review by the Independent National Security Legislation Monitor (INSLM) of the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* (SLAID Act).

2. Consistent with established practice, the Inspector-General does not comment on the policy rationale underlying legislation. Rather, this submission discusses the key features of the relevant provisions that relate to oversight and the outcomes of the IGIS's oversight work regarding the exercise by the Australian Federal Police (AFP) and the Australian Criminal Intelligence Commission (ACIC) of their powers and functions pursuant to Part 2 Division 6 of the *Surveillance Devices Act 2004* (SD Act).

Background

About the Inspector-General

3. The Inspector-General is an independent statutory officer appointed under the *Inspector-General of Intelligence and Security Act 1986* (Cth) (IGIS Act).[1]

4. Under his existing jurisdiction, the Inspector-General reviews the activities of the following six intelligence agencies:

    - Office of National Intelligence (ONI)
    - Australian Security Intelligence Organisation (ASIO)
    - Australian Secret Intelligence Service (ASIS)
    - Australian Signals Directorate (ASD)
    - Australian Geospatial-Intelligence Organisation (AGO)
    - Defence Intelligence Organisation (DIO)

5. In addition, the Inspector-General has limited jurisdiction for the intelligence functions of the Australian Criminal Intelligence Commission (ACIC) and the Australian Federal Police (AFP), as defined in the IGIS Act.[2]

6. The overarching purpose of the Inspector-General's functions is to assist Ministers in the oversight and review of the activities of each intelligence agency to ensure that they are legal and proper, comply with ministerial guidelines and directions, and respect human rights.[3]

Surveillance Legislation Amendment (Identify and Disrupt) Act 2021

7. The Office of the Inspector-General of Intelligence and Security (the IGIS) notes the breadth of questions raised in Issues Paper of 7 November 2024 (Issues Paper) which has been released to the public for consultation. As the IGIS jurisdiction is confined to the use of

---

[1] *The purposes of the IGIS include the functions of the Inspector-General referred to in sections 8, 9 and 9A of the IGIS Act (paragraph 6AA(e) IGIS Act).*

[2] *The intelligence functions of the ACIC and AFP, as defined in section 3 of the IGIS Act, are the collection, correlation, analysis, production and dissemination of intelligence obtained by the ACIC or AFP from the execution of a network activity warrant; or the performance of a function, or the exercise of a power, conferred on a law enforcement officer of ACIC or AFP by the network activity warrant provisions of the Surveillance Devices Act 2004.*

[3] *See section 4 IGIS Act.*

Network Activity Warrants by the ACIC and AFP this submission is similarly confined to the oversight of that particular warrant.

8. This submission touches on three subject areas in response to the matters raised in the Issues Paper. These are the jurisdictional split between the IGIS and the Office of the Commonwealth Ombudsman in respect of the three warrant types created by the SLAID Act, the powers and functions necessary to effectively oversight Network Activity Warrants, and transparency and public reporting requirements.

Jurisdiction split between oversight bodies

9. The IGIS's oversight jurisdiction of the individual warrants contained in the SLAID Act includes the consideration of both the legality and propriety of agency activities[4]. The Ombudsman is able to inspect legal compliance with the SD Act[5], the *Crimes Act 1914*[6], and administrative best practice[7] in relation to the SLAID Act warrant types. The IGIS notes that, as flagged by the issues paper itself[8], this suggests that among the three warrant types the Issues Paper covers there is some variation in the nature of their oversight.

10. To date, the IGIS has not identified any immediate practical concern with the division of responsibilities, the potential variation in the nature of oversight, nor with its own ability to undertake oversight in accordance with the nature or scope of the IGIS jurisdiction.

11. The IGIS has undertaken 4 inspections of the AFP's use of Network Activity Warrants and 4 inspections of the ACIC's use of Network Activity Warrants since both were able to request such warrants in 2021. Based on its oversight activities to date, the IGIS's has identified and provided value by attention to the additional lens of propriety (and human rights).

12. Overall, the IGIS has found a high degree of compliance with legislative requirements. The IGIS has identified a very small number of instances where the relevant agency had not provided a required notification to the IGIS in a timely manner or had not provided sufficient information to meet its reporting obligations in its report to the relevant Minister. The IGIS did not consider these as systemic issues. The IGIS has provided a small number of recommendations to improve the ability to demonstrate and manage compliance.

13. If the Intelligence Services Legislation Amendment Bill 2023 (ISLAB) is implemented in its current form, the scope of the IGIS's oversight will expand to include all ACIC activities and the 'intelligence functions' of the AFP. This will see the IGIS having oversight responsibility for all warrant types under the SD Act for the ACIC, but only certain instances of each warrant type for the AFP. For instance, if the AFP seeks a Data Disruption Warrant (DDW) (or any warrant type under the SD Act) for a non-intelligence function, oversight responsibility will fall to the Ombudsman to review based on their oversight authorities. However, if the warrant is for the purpose of undertaking an intelligence function, oversight responsibility will rest with the IGIS under the IGIS Act.[9]

14. The SLAID Act information sharing provisions between the IGIS and the Ombudsman were introduced to 'ensure that the risk of duplication of oversight between the IGIS and the

[4] *See section 4 IGIS Act.*
[5] *SD Act s 55.*
[6] *Crimes Act 1914 s 3ZZVR.*
[7] *Commonwealth Ombudsman, Submission No 5 to the PJCIS, Review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 (February 2021) 2.*
[8] *Issues Paper - Data Disruption, Network Activity and Account Takeover Warrants – Review of Surveillance Legislation Amendment (Identify and Disrupt) Act 2021 (SLAID Act)* pages 52-54.
[9] *Ombudsman Act s 5; ISLAB item 11.*

Ombudsman is appropriately managed and minimised'.[10] The current information sharing provisions available to the IGIS appear sufficient whilst noting that there has been no need to make use of them to date in respect of Network Activity Warrants.

Powers and functions to undertake oversight

15. The IGIS Act provides sufficient powers and functions in relation to the effective oversight of Network Activity Warrants.

16. In particular, the IGIS notes that 2023 amendments to the IGIS Act provided additional clarity in respect of the IGIS's powers to remove and copy documents as well as better define access arrangements to agency facilities.[11] This additional clarity has provided inspection teams with additional surety in the conduct of their work. Similar provisions are currently being considered in the context of preliminary inquiries.[12]

17. Notification to the IGIS is required of the AFP and ACIC in the event that a network activity warrant is issued, extended, varied, revoked or a concealment of activities is undertaken.[13] This notification is required within 7 days of occurrence. Notwithstanding the aforementioned non-compliance identified with notification timeframes, the IGIS finds this timeframe appropriate for the purpose of enabling it to fulfil its oversight responsibilities in relation to network activity warrants.

18. While the notification timeframe is appropriate, the SD Act is not clear in what material is required to be provided with these notifications. The IGIS has found the information provided varies between the agencies. While additional detail is able to be requested, access to the appropriate material in a timelier manner, without the need to request it, would assist timely and effective oversight. Accordingly, there may be benefit in clarifying the intended content of the required notifications (for example explicitly requiring agencies to provide a copy of the warrant and supporting affidavit with the notification).

Transparency and public reporting

19. Currently the reporting requirements of the AFP and the ACIC to report to the Minister only at the conclusion of a network activity warrant or a data disruption warrant, 'as soon as practical' allows for a degree of inconsistency across reporting requirements.[14]

20. Additionally, noting that warrants can be issued for a 90-day period and subsequently extended an unlimited amount of times for additional 90-day periods there may be an extended period of time in which the Minister is not being provided any substantive information about the execution of the warrant.

21. There may be benefit in considering a more definite timeframe for reporting at the conclusion of the warrant or when they are renewed.

---

[10] IGIS, Submission No 18 to PJCIS, Review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 (26 February 2021) 6 [14]. See also Commonwealth Ombudsman, Submission No 5 to the PJCIS, Review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 (February 2021) 2 [13]. Under the SD Act and the Crimes Act, 'protected information' can be shared to an Ombudsman or IGIS official for the purposes of them exercising their powers or performing functions or duties: see, e.g., SD Act ss 45(6A), 45B(8).

[11] Inspector-General of Intelligence and Security and Other Legislation Amendment (Modernisation) Act 2023

[12] Oversight Legislation Amendment (Robodebt Royal Commission Response and Other Measures) Bill 2024

[13] SD Act s 27KM(3), ss 27KQ(7), 27KR(6)-(7), 49D.

[14] SD Act s 49(1)(c) and s 50(3)