Australian Government
Independent National Security Legislation Monitor

Independent National Security Legislation Monitor
3-5 National Circuit
Barton ACT 2600
Tel: (02) 6141 4590

7 April 2026

Senator Jana Stewart
Chair
Senate Legal and Constitutional Affairs Legislation Committee
PO Box 6100
Parliament House
Canberra ACT 2600

Dear Chair

Crimes and Other Legislation Amendment (Omnibus No. 1) Bill 2026

I welcome the opportunity to make this submission to the review by the Senate Legal and Constitutional Affairs Legislation Committee (the Committee) of the Crimes and Other Legislation Amendment (Omnibus No. 1) Bill 2026 (the Bill).

This submission comments on aspects of the Bill that relate to my recently completed review of the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* (Cth) (SLAID Act). My report for this review, *Data Disruption, Network Activity and Account Takeover Powers: Review of Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* (attached for information and also available on the INSLM website) was tabled on 1 September 2025 (INSLM SLAID Act Report).

In its November 2025 response, the Government agreed to four recommendations, agreed two in part, and noted the remaining 15. It indicated that the recommendations agreed in part or noted would be considered further as part of broader electronic surveillance reforms, given their relevance to the legal framework for surveillance as a whole.

There is a strong case for maintaining network activity, data disruption, and account takeover warrants powers along with emergency authorisations, as they have been effective in helping to identify and disrupt serious crime, including where other powers would have been ineffective.

However, these warrants should only be retained if significant improvements are made to the system for issuing them. It is essential that changes to improve the safeguards for these warrants are brought forward as a matter of priority.

I support amendments contained in Division 3 of Schedule 1 of Part 3 to the Bill removing data disruption powers from the Australian Criminal Intelligence Commission (ACIC). This is an important change. Data disruption should be a 'last resort' measure to disrupt serious crime, and their use should be restricted to the Australian Federal Police (AFP) only. Covert disruption of data on devices inside Australia is not an intelligence function, it should only be exercised if the full suite of available law enforcement options is available to the relevant agency and the use of these other available powers has been considered first.

Potential changes to ACIC network activity and account takeover warrants have been flagged in connection with another Bill. This means that an extension to the sunset clause in the current Bill could be affected by subsequent change to the scope or thresholds for these warrants.

Extending legislative sunset of DDW, ATW and NAW warrants

Among other changes, Part 3 of Schedule 1 of the Bill would extend the sunset date for network activity warrants (NAW), data disruption warrants (DDW), account takeover warrants (ATW), and related emergency authorisations given to the AFP and ACIC by 3 years to 4 September 2029 in the *Surveillance Devices Act 2004* (Cth) (SD Act) and *Crimes Act 1914* (Cth) (Crimes Act).[1]

In the INSLM SLAID Act report, I found that these powers have been used rarely but effectively against serious cyber-enabled and cyber-dependant crime, helping agencies gather intelligence and preserve evidence in ways traditional methods cannot. However, while they remain necessary, I also found that these powers should only be retained with stronger safeguards.

Importantly, my support for the retention of DDWs, NAWs and ATWs was conditional on changes being made to improve issuing arrangements to introduce a new system with three core elements: retired judges as the issuing authorities; public interest monitors; and access to independent technical advice (**Recommendations 6-8** of the INSLM SLAID Act report).

The EM states the amendments contained in the Bill partially implement recommendations from my review while leaving broader reforms to electronic surveillance powers under consideration:

> [t]hese amendments would give effect to aspects of the Independent National Security Legislation Monitor's Review of the Surveillance Legislation Amendment (Identify and Disrupt) Act 2021, while the Government is considering the broader framework for the powers, and other recommendations in the Monitor's Review, as part of electronic surveillance reforms.[2]

It is disappointing that consideration of holistic electronic surveillance reforms has taken so long. The electronic surveillance review is a long over-due reform of police, security and intelligence agency electronic surveillance powers. The current electronic surveillance review was initiated in response to principles for reform set out in the *2019 Comprehensive Review of the Legal Framework of the National Intelligence Community*, conducted by Mr Dennis Richardson AC.[3] I consider the modernisation of surveillance and cyber security powers along with their safeguards to be urgent and am concerned that it is considered necessary to extend the current sunset to late 2029 to await those reforms.

Removing DDWs from ACIC

Schedule 1 of the Bill would also remove the ACIC's ability to obtain DDWs. This is an important change. In the INSLM SLAID Act report, I explained that DDWs should be a 'last resort' measure to disrupt serious crime and their use should be restricted to AFP only. Undertaking an otherwise unlawful activity to disrupt crime is an extension of the law enforcement function of police. Although ACIC's intelligence activities may incidentally have a disruptive effect, engaging in otherwise unlawful disruption should not form part of its legislative remit, which is focused on intelligence collection and analysis. This position has also been supported in previous reviews of ACIC's powers.[4]

---

[1] Currently, *Crimes Act* s 3ZZUMA, *SD Act* s 27KAA and *SD Act* s 27KKA provide that ATWs, DDWs and NAWs will each sunset 5 years after commencement.
[2] Explanatory Memorandum, 5 [5].
[3] Dennis Richardson, *Report of the Comprehensive Review of the Legal Framework of the National Intelligence Community* (Final Report, December 2019) vol 2, 268 Recommendation 75.
[4] Stephen Merchant and Greg Wilson, *Independent Review of the Australian Criminal Intelligence Commission and associated Commonwealth law enforcement arrangements* (Report, May 2024) 31-32 Recommendation 9.

Technical changes

If the sunset for DDW, ATW and NAWs is to be extended, there are certain technical changes that must be addressed to avoid unintended operational consequences. These are in the Bill and should be supported.

- Where the powers are extended, the Bill includes transitional and saving provisions to avoid unintended operational consequences, including clarifying that concealment activities and warrant conditions can continue after the sunset period (4 September 2026) for warrants that have already been executed.[5] For context, concealment powers enable the AFP and ACIC to do a wide range of things 'reasonably necessary' to conceal the fact that anything has been done under the warrant.[6]
- It also ensures that information lawfully obtained under existing warrants is treated as protected information so it can continue to be used and disclosed in accordance with the legislation, even after the powers themselves have ceased.[7] For example, currently, information obtained under a NAW is subject to more restrictions on use and disclosure than information obtained under other warrants. The main restriction is that, in general, 'protected NAW information' may not be used, recorded, communicated, published or admitted in evidence in criminal proceedings.[8] This is consistent with NAWs being an intelligence warrant, subject to a lower threshold and potentially much wider in scope than other criminal warrants. It also ensures that sensitive capabilities and methods are not disclosed in court.

These transitional provisions are critical to ensuring safeguards applicable to warrant powers and the use and disclosure of information obtained under a warrant (prior to sunset) continue to apply.[9]

Other changes made by the Bill

Other schedules of the Bill make changes to other law enforcement powers and criminal law procedure, these are not matters that I have reviewed and I make no comment on these aspects.

Related legislation may affect powers being extended

The Bill does not make any substantive changes to the provisions governing ATW and NAW warrant and emergency authorisation powers. However, the Australian Criminal Intelligence Commission Bill 2026 (ACIC Bill), introduced on 25 March 2026 and referred to the Parliamentary Joint Committee on Intelligence and Security, makes significant changes to the legislative remit of ACIC. The Explanatory Memorandum to the ACIC Bill indicates that a consequential and transitional amendment package to

---

[5] Schedule 1 Item 16(7)-(8) (concealment of access for ATWs); Item 30(8)-(9) and 31(4)-(5) (concealment of access for DDWs); Item 33(4)-(5) (concealment of access for NAWs).
[6] *Crimes Act* s 3ZZUR(6)-(8); *SD Act* s 27KE(9)-(12), 27KP(8)-(10).
[7] Schedule 1 Item 17 (protected information for ATWs); Item 34 (protected information for NAWs).
[8] *SD Act* s 45B(1); protected NAW information may be admitted in evidence in a prosecution for a protected NAW information secrecy offence and a proceeding that is not a criminal proceeding: s 45B(10).
[9] For example, statutory conditions on ATWs that the warrant must not be executed in a manner that results in loss or damage to data unless the damage is justified and proportionate, having regard to the alleged relevant offence in respect of which the warrant is issued and prohibition on permanent loss of money or property: *Crimes Act* s 3ZZUR(8)(a) and (b).

the ACIC Bill will be introduced subsequently to align ACIC warrant powers in the Crimes Act and SD Act with its new remit to obtain intelligence in respect of a matter that is important in relation to combatting serious and organised crime.[10] This suggests that changes may be made to the ATW and NAW powers as they apply to the ACIC. If this is the case, then the extension of the sunset clause being considered by your Committee in the current Bill will potentially be affected by subsequent changes to the scope and thresholds for the use of those extended powers.

I was supportive of changes to the ACIC's ATW thresholds to reflect its intelligence functions (**Recommendation 3** of the INSLM SLAID Act report).[11] However, whether the proposed changes achieve this in a proportionate way will be dependent on the nature of the amendments in the yet to be introduced consequential and transitional amendment package.

Please let me know if the Committee requires further information about my recent review of the SLAID Act and the importance of these amendments. The best point of contact for my office is inslm@inslm.gov.au.

Yours sincerely

[redacted]

Jake Blight
Independent National Security Legislation Monitor

[10] See for example, new thresholds for ACIC search warrants: Australian Criminal Intelligence Commission Bill 2026, cl 157(1) read alongside new definition of 'serious and organised crime' cl 10. See also, Explanatory Memorandum, 3 and 284-285.
[11] Stephen Merchant and Greg Wilson, *Independent Review of the Australian Criminal Intelligence Commission and associated Commonwealth law enforcement arrangements* (Report, May 2024) 25 Recommendation 4.

Australian Government
Independent National Security Legislation Monitor

Data Disruption, Network Activity and Account Takeover Powers

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

INSLM
Jake Blight

Independent National Security Legislation Monitor (INSLM) Report

Data Disruption, Network Activity and Account Takeover Powers

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

978-1-921357-45-9 (Print)

978-1-921357-46-6 (Online)

Copyright

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (www.dpmc.gov.au/government/commonwealth-coat-arms).

Acknowledgement of Country

The Independent National Security Legislation Monitor and the INSLM Office acknowledge the custodians of the lands on which we work and their contribution to our communities. We pay our respect to Elders past and present, and extend this respect to Aboriginal and Torres Strait Islander people across this nation, who hold the memories, traditions, cultures and hopes of Aboriginal and Torres Strait Islander peoples.

Through our reviews and recommendations, the Monitor and INSLM Office seek to ensure Australia's national security and counter terrorism legislation remains proportionate to the threats these laws were designed to address and achieves an appropriate balance between national security and individual rights. As an organisation focused on law and law reform, we acknowledge that Aboriginal and Torres Strait Islander peoples have had a continuing system of law on these lands for tens of thousands of years.

Australian Government
Independent National Security Legislation Monitor

31 July 2025

The Hon Michelle Rowland MP

Attorney-General

Parliament House
CANBERRA ACT 2600

Dear Attorney-General,

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

Pursuant to s 6(1E) of the *Independent National Security Legislation Monitor Act 2010* (Cth) (*INSLM Act*), I have reviewed the operation, effectiveness and implications of the amendments made by Schedules 1, 2 and 3 to the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* (Cth).

In my view, this report does not contain information of the kind referred to in s 29(3) of the *INSLM Act* and is suitable to be laid before both Houses of Parliament.

Yours sincerely,

[redacted]

Jake Blight

Independent National Security Legislation Monitor

Public consent to intrusive laws depends on people trusting the authorities, both to keep them safe and not to spy needlessly on them. This in turn requires knowledge at least in outline of what powers are liable to be used, and visible authorisation and oversight mechanisms in which the wider public, as well as those already initiated into the secret world, can have confidence.

Lord Anderson of Ipswich, Former United Kingdom Independent Reviewer of Terrorism Legislation

The issuing stage is the most critical point for the appropriate balance to be struck between security and rights.

Associate Professor Rebecca Ananian-Welsh, Associate Professor Tamara Tulich, Dr Keiran Hardy, Professor Peter Greste, Dr Ausma Bernot & Associate Professor Danielle Ireland-Piper

Table of Contents

Executive Summary

Australia faces a significant and persistent threat from cyber-dependent and cyber-enabled crime – that is, crime directed at and enabled by computers. The *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* (Cth) (*SLAID Act*) introduced new powers aimed at helping to address some of the challenges of policing this type of crime.

Under the *SLAID Act*, the Australian Federal Police (AFP) and the Australian Criminal Intelligence Commission (ACIC) gained access to 3 new warrant types: **the data disruption warrant** (DDW), which allows AFP and ACIC to modify, add, copy or delete data to disrupt online crime; the **network activity warrant** (NAW), which allows AFP and ACIC to collect intelligence about a 'criminal network of individuals' or anyone electronically connected to that network; and the **account takeover warrant** (ATW), which allows AFP and ACIC to take control of a person's online accounts to gather evidence. The *SLAID Act* also introduced a requirement that the Independent National Security Legislation Monitor commence a review of the new powers within 3 years of the day the Act received royal assent.

The new powers have been effective in helping to identify and disrupt serious crime, including in cases where other powers would have been ineffective, so there is a strong case for maintaining them. However, the powers are extraordinary and invasive and so it is essential that the safeguards are fit for purpose and operating effectively. DDWs allow otherwise unlawful action to be taken on computers in Australia for the sole purpose of disruption (not surveillance and future prosecution) and without any prior criminal or civil proceeding. NAWs allow surveillance of whole networks of people to gather intelligence 'relevant' to crime, but without a requirement to have a reasonable suspicion that all those under surveillance are engaged in criminal activity. An ATW can effectively lock a person out of their online account.

The review found that **the main safeguard, the current system for issuing warrants, is not fit for purpose**. This is largely because the current system is based on a process designed over a century ago for basic property search warrants. Unlike those early warrants, *SLAID Act* warrants involve the use of advanced technical capabilities and can give agencies access to large amounts of information about many people from many computers. The information that is collected can quickly be shared with police and intelligence agencies nationally and internationally. Moreover, unlike earlier warrants, which were overt, the warrants are usually covert – they are usually used without the knowledge of those who are affected. The information that is collected under them is rarely used in evidence, so a person affected by a warrant effectively has no recourse to judicial review.

The review found that, in practice, *SLAID Act* warrants are issued by a small number of Administrative Review Tribunal (ART) members who volunteer to do so in their 'personal capacity' on top of their busy workload. They do not have access to relevant training, independent technical advice, submissions on matters of public interest or feedback from oversight processes. Few have experience in criminal law matters. Time taken to issue warrants is contributing to a growing backlog of administrative review cases in the ART. This arrangement for issuing warrants is **inadequate and unsustainable**.

This review proposes a new system for issuing warrants. The system consists of three core elements: a panel of retired judges as the issuing authorities; public interest monitors; and access to independent technical advice. Use of retired judges relieves the burden on the ART and courts and draws on the expertise and gravitas of judges. Public interest monitors would play a dual role: pre-review of warrant applications to provide feedback on areas of concern; and the ability to make submissions on matters of public interest and draw attention to any relevant oversight findings. Technical advisers would assist by giving independent advice on the risk and reach of warrants when required. This new system will engender more public confidence and put the decision-maker in a much better position to provide robust independent scrutiny. Having dedicated issuing authorities should make it easier for applicants to seek a decision, including for urgent matters out of hours. Based on the experience of other jurisdictions, public interest monitors would not cause delay and would improve applications.

The review also recommends other improvements, including a statutory duty of candour and a mechanism to ensure that applicants cannot choose which decision-maker assesses their proposed warrant.

Subject to the introduction of a new system for issuing warrants based on the identified key features, I recommend that *SLAID Act* warrants be retained. DDWs should be a 'last resort' measure to disrupt serious crime and their use should be restricted to AFP only. ACIC is a criminal intelligence agency and should be able to access ATWs for intelligence (not evidence) purposes. The greater safeguards provided by the proposed new system for issuing warrants allows for **some expansion to *SLAID Act* powers**: NAWs should be available for up to 6 months and named person ATWs should be introduced. Emergency authorisations and assistance orders should be retained with minor changes.

SLAID Act warrants should only be available for crimes punishable by 5 or more years imprisonment. The proposed new system for issuing warrants provides the opportunity to both strengthen and significantly streamline the currently **complex and overlapping issuing criteria**. The current **secrecy provisions should be replaced**. They are unreasonably complex and inconsistent. Changes are needed to ensure that secrecy offences do not stop potentially exculpatory material from being disclosed in a prosecution or prevent those served with an assistance order from seeking legal advice.

When assessing the proportionality of a warrant, it is necessary to consider the whole **'life cycle of data'**: collection, use, dissemination and retention. It is important that this incorporates protections for sensitive categories of data, such as information about journalists' sources or that is subject to legal professional privilege (including when collected incidentally). The effectiveness of policies and administrative guidance across the full life cycle of data should be considered when issuing warrants.

I recommend some **improvements to ministerial and public reporting** to facilitate oversight and accountability and as much transparency as is possible about the use of covert powers. **Oversight can be improved**, including by replacing prescriptive requirements for inspections by the Commonwealth Ombudsman with a more flexible mandate. There is also opportunity to move detailed reporting and notification requirements out of the *SLAID Act* and into more readily updateable binding administrative guidance.

Implementation of the recommendations in this review will improve Australia's compliance with **international human rights obligations** including the right to privacy and the right to a fair trial. International norms and obligations about the extraterritorial use of law enforcement powers in cyberspace are evolving. At this time there was not a sufficient case to recommend any change to the requirement for consent to be obtained for extraterritorial effects, especially for DDWs.

This review benefited greatly from the 31 submissions and supplementary submissions, 2 days of public hearings, 3 private hearings and many consultation meetings. I thank all individuals, organisations and agencies who engaged with this review: your input was valuable and I hope that is reflected in this report. This major review was completed in 12 months with a review team consisting of 3 staff; this review would not have been possible without my hardworking team, thank you.

Recommendations

No.	Issue	Recommendation
1	**Retention of DDWs**	AFP should retain DDWs, subject to recommendations 6–8 being implemented. ACIC should not retain the ability to use DDWs.
2	**Retention of NAWs**	ACIC and AFP should retain NAWs, subject to recommendations 6–8 being implemented.
3	**Retention of ATWs**	Both ACIC and AFP should retain ATWs, subject to recommendations 6–8 being implemented. In the case of ACIC, ATWs should be for intelligence rather than evidence collection purposes.
4	**Named person ATWs**	Named person ATWs should be introduced for AFP and ACIC, subject to recommendations 6–8 and the following additional safeguards: **a)** Available only where the use of an account-based ATW would be ineffective. **b)** A certification process for adding accounts based on the same criteria used to issue ATWs. **c)** Additional record keeping and reporting requirements.
5	**Maximum duration of NAWs**	The maximum duration of NAWs should be extended to 6 months, subject to recommendations 6–8 and a mechanism to ensure 6 monthly reporting.
6	**Issuing authorities**	The issuing authorities should be retired judges. If this is not accepted then it should be current judges for all *SLAID Act* warrants. In either case they must be supported by PIMs and technical advisors.

No.	Issue	Recommendation
7	**Introduce PIMs**	There should be Public Interest Monitors whose role includes providing submissions on matters of public interest and feedback from oversight processes, identifying matters where independent technical advice may be required and providing comments on draft warrant applications and templates.
8	**Other improvements to issuing system**	The warrant issuing system also requires: **a)** A mechanism for access to independent technical advice. **b)** A statutory duty of candour requiring disclosure of all matters of which the applicant is aware, both favourable and adverse. **c)** That warrant applications are independently allocated to issuing authorities. **d)** An effective secretariat should be established with functions that include the allocation of warrants, case management and data collection.
9	**Relevant offence threshold**	Warrants should only be available for offences punishable by 5 or more years imprisonment.
10	**Criminal network of individuals**	The expression 'criminal network of individuals' should be renamed 'targeted network' or something similar that does not misleadingly imply that all persons using the same electronic service are suspected of being engaged in criminal activity.
11	**Urgent applications**	For urgent applications the issuing authority should be satisfied that there is a reasonable basis for both the 'impracticality' and the 'urgency' criteria.

No.	Issue	Recommendation
12	**Simplified issuing criteria**	Issuing criteria should require that the issuing authority is satisfied that the warrant is necessary and proportionate in all the circumstances. In assessing necessity and proportionality, the list of matters to be considered should include the: **a)** nature and gravity of the offences being investigated (or disrupted); **b)** likelihood that the proposed activity will succeed as well as the likely value of the resulting intelligence, evidence or disruption; **c)** extent to which the privacy of any person is likely to be interfered with; **d)** extent to which property rights are likely to be interfered with, including through introduction of vulnerabilities; **e)** likelihood of special categories of information *including* information subject to LPP and information about journalists' sources being collected and, if it is, how the information will be protected; and **f)** existence of any alternative, less intrusive means of obtaining the information.
13	**DDWs as a last resort**	DDWs should only be available when other measures would not be effective.

No.	Issue	Recommendation
14	**Simplifying secrecy, use and disclosure**	The secrecy provisions should be reformed in accordance with the following principles: **a)** Removal of unnecessary complexity and inconsistency. **b)** Reliance on the general secrecy offences in the *Criminal Code.* **c)** Retention of strict limits on the way officials can use information obtained under warrants, potentially through positively defining what use is permitted in the 'course of duties'. **d)** There should be no barrier to a person seeking legal advice about an assistance order they may be required to comply with. **e)** Potentially exculpatory material obtained under a NAW should be able to be disclosed in accordance with the usual prosecutorial duty of disclosure. **f)** The law should be clarified to put beyond doubt that NAW information cannot be admitted in evidence in proceedings under the *Proceeds of Crime Act 2002* (Cth).
15	**Retention and review**	Information accessed under a *SLAID Act* power should be reviewed at least every 5 years and destroyed if no longer required for identified purposes. Internal agency policies and/or binding administrative guidance should make provision for earlier reviews of particularly sensitive categories of information.
16	**Administrative guidance for lifecycle of data**	Further consideration should be given to issuing binding administrative guidance to provide additional protections for the collection, use, retention and disclosure of information, particularly personal and sensitive information.

No.	Issue	Recommendation
17	**Emergency authorisations**	The scheme for emergency authorisations should be amended so that: **a)** Emergency authorisations are not available to ACIC. **b)** The limitation preventing an issuing authority from ever requiring the destruction of information should be removed.
18	**Assistance Orders**	The scheme for assistance orders should be modified so that: **a)** Assistance orders are only be able to be issued when it is proportionate to do so. **b)** Issuing authorities have express authority to place limits or conditions on assistance orders.
19	**Ministerial reporting requirements**	Ministerial reporting requirements should be retained and amended so that: **a)** There are consistent reporting requirements across the *SLAID Act* warrants. **b)** Reporting on named person ATWs includes details of the accounts that were taken over under the warrant and the reasons it would not have been effective to take over those accounts under a specified account ATW. **c)** There is no more than 6 months between the warrant being issued and the requirement to provide a report to the Minister being triggered. **d)** Individual reports on ATWs are required.

No.	Issue	Recommendation
20	**Public annual reporting**	Public annual reporting requirements should be amended to include: **a)** The number of warrants where specified categories of sensitive information is sought or is likely to be obtained (including LPP and journalist source information). **b)** The number of people, devices and accounts affected by each category of warrant (NAW, DDW and ATW). **c)** Reasons for refusal of an ATW (consistent with the existing requirement for DDWs and NAWs). **d)** The number of occasions on which issuing authorities have required agencies to provide further information in support of warrant applications; the number of warrants granted with conditions; input of Commonwealth PIMs in warrant issuing; and, the work of the technical advisors. **e)** The number of assistance orders sought, granted and used each year. **f)** An annual statement that describes, as far as possible, how the use of each type of warrant has enhanced the ability of each agency to investigate, disrupt and prosecute (as relevant) serious crime. **g)** A framework for deferred reporting based on that in s 50A of the *SD Act*.

No.	Issue	Recommendation
21	**Oversight arrangements**	Oversight arrangements should be modified to reflect the following: **a)** There should be no statutory barrier to IGIS, the Ombudsman, PIMs and the technical advisors sharing relevant information. **b)** Oversight bodies and the INSLM should have access to the proposed technical advisors. **c)** Existing prescriptive requirements for Ombudsman inspections should be repealed and replaced by the ability to conduct inspections to examine matters akin to those that the Ombudsman can currently consider in 'investigations'. **d)** Prescriptive statutory record keeping and notification requirements should be replaced by a scheme that allows for binding administrative guidance to be given and updated as required. **e)** IGIS and the Ombudsman should be able to brief parliamentary committees and IGIS should be able to publish unclassified inspections reports and inquiries at any time. **f)** There should be consistent obligations on the Ombudsman to not include sensitive DDW or ATW information in public reports.

Part 1. Scope, powers and threat

This is a report of an independent review of the amendments made by schs 1, 2, and 3 of the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* (Cth) (*SLAID Act*). The review was required by, and conducted under, the *Independent National Security Legislation Monitor Act 2010* (Cth) (*INSLM Act*).

The report is set out in 7 parts covering each of the main areas examined in this review. Each part comprises several chapters addressing particular matters within a given subject area. Part 1 begins with an explanation of this review's scope and gives an overview of other recent or ongoing law reform processes relevant to the *SLAID Act*. It then introduces the *SLAID Act* powers under examination and the threat environment in which they operate.

The *SLAID Act* warrants are unique, indeed they were described as 'world-leading and novel' when introduced.[1] These warrants were intended to assist police and criminal intelligence agencies to address new and growing threats associated with cyber-enabled and cyber-dependent serious crimes. Data disruption and account takeover powers are not properly characterised as electronic surveillance powers – they permit more than surveillance and are more rights-intrusive than electronic surveillance or search powers. Network activity warrants are unique amongst electronic surveillance powers, as they have a much lower threshold for issuing and permit much wider surveillance.

The system used for issuing warrants has changed little in the last century. It was originally designed for physical search warrants. Those original warrants were overt, so they could feasibly be challenged through the courts. Physical searches – how they were conducted, the amount of information that could be collected under them and how that information could be stored and distributed – bear no resemblance to modern warrants in terms of what can be authorised or the technology that underpins them. A key theme of this review is whether the system for issuing warrants remains fit-for-purpose for modern warrants like those introduced by the *SLAID Act*. This theme is briefly introduced in this Part and is further discussed in Part 3 of this report.

[1] Parliamentary Joint Committee on Intelligence and Security (PJCIS), Parliament of Australia, *Advisory report on the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (Report, August 2021) 119 [6.1] (*PJCIS SLAID Report*).

Chapter 1: Scope and context for this review

1.1 The Monitor is a statutory office holder who independently reviews Australia's national security and counterterrorism laws and can make recommendations for law reform. The Monitor's position, functions and powers are established by the *INSLM Act*.[2]

1.2 The Monitor can initiate certain reviews of their own motion or have a matter referred by the Prime Minister, the Attorney-General or the Parliamentary Joint Committee on Intelligence and Security (PJCIS). The *INSLM Act* also requires the Monitor to undertake certain reviews.[3] The Monitor's reviews consider the operation, effectiveness and implications of the relevant law and whether it contains appropriate protections for individual rights, remains necessary and proportionate, and is consistent with Australia's international obligations.[4]

1.3 The Monitor has powers to access any material they consider relevant, including classified information, and can determine their own review process. Briefly, the process for this review involved the publication of an issues paper, extensive consultation, receipt and consideration of 31 submissions and supplementary submissions (including 2 classified submissions), 2 days of public hearings and 3 private hearings. The process of this review is described in more detail in Annex A.

Requirement for this review

1.4 The Surveillance Legislation Amendment (Identify and Disrupt) Bill 2021 (Cth) (SLAID Bill) was introduced to Parliament on 3 December 2020. The Revised Explanatory Memorandum for the SLAID Bill said it was introduced to address challenges involved in the use of technologies that frustrate or inhibit the ability of the Australian Federal Police (AFP) and the Australian Criminal Intelligence Commission (ACIC) to perform their respective functions.[5] The SLAID Bill was passed by both houses by 25 August 2021 and received royal assent on 3 September 2021. Each of the warrant powers introduced by the *SLAID Act* are due to sunset on 4 September 2026.[6]

1.5 The SLAID Bill was considered by 3 parliamentary committees: the PJCIS,[7] the Senate Standing Committee for the Scrutiny of Bills[8] and the Parliamentary

2 *Independent National Security Legislation Monitor Act 2010* (Cth) (*INSLM Act*).
3 *INSLM Act* ss 6–7A.
4 *INSLM Act* ss 6(1), 8.
5 Revised Explanatory Memorandum, Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 (Cth) 2 (Revised Explanatory Memorandum).
6 *Crimes Act 1914* (Cth) s 3ZZUMA (*Crimes Act*); *Surveillance Devices Act 2004* (Cth) ss 27KAA, 27KKA (*SD Act*). This was consistent with recommendation 8 of the *PJCIS SLAID Report*.
7 *PJCIS SLAID Report*.
8 Senate Standing Committee for the Scrutiny of Bills (Scrutiny of Bills Committee), Parliament of Australia, *Scrutiny Digest* (Digest No 1 of 2021, 29 January 2021); Scrutiny of Bills Committee, *Scrutiny Digest* (Digest No 5 of 2021, 17 March 2021).

Joint Committee on Human Rights (PJCHR).[9] Collectively the committees made 35 recommendations.[10] While not all committee recommendations were accepted, 60 government amendments were made to the Bill before it was passed.

1.6 Those amendments included implementing a PJCIS recommendation that the Monitor be required to commence a review of the new powers within 3 years of the day they receive royal assent.[11] In accordance with that requirement, this review commenced in July 2024.[12]

The *SLAID Act* mandated that an INSLM review commence within 3 years.

1.7 This review of the *SLAID Act* amendments must consider the operation, effectiveness and implications of the relevant amendments.[13] In doing so, this review also considers the appropriateness of safeguards to protect the rights of individuals and whether the laws remain necessary and proportionate to the current threats. I have also had regard to Australia's obligations under international agreements on human rights and cybersecurity.[14]

1.8 The *SLAID Act* also made an amendment enabling the PJCIS, at its discretion, to commence a review of the operation, effectiveness and implications of the amendments made by schs 1–3 of the *SLAID Act* after 3 September 2025.[15] The PJCIS previously recommended that this potential review should be timed 'to allow the Committee to take into account any report by the INSLM.'[16] I have managed my review to ensure it is completed in time for the PJCIS to take my report into account in deciding whether it wishes to do another review and to consider any legislative response the government proposes before the provisions sunset on 4 September 2026.

Other related reviews and inquiries

1.9 At the time this report is made, a number of related reviews and inquiries were recently completed or are ongoing. In addition to the submissions and evidence provided to this review, information from other related reviews has informed my review process. The related reviews and inquiries include an ongoing project to reform Australia's electronic surveillance framework; a recent *Independent review of the Australian Criminal Intelligence Commission and associated Commonwealth law*

9 Parliamentary Joint Committee on Human Rights (PJCHR), Parliament of Australia, *Human Rights Scrutiny Report* (Report No 1 of 2021, 3 February 2021); PJCHR, *Human Rights Scrutiny Report* (Report No 3 of 2021, 17 March 2021).

10 The Scrutiny of Bills Committee also requested an addendum to the Explanatory Memorandum to include detail that the Minister provided on questions and concerns the committee raised.

11 *PJCIS SLAID Report* 130 [6.49]–[6.50]; *INSLM Act* s 6(1E).

12 Independent National Security Legislation Monitor (Cth), 'Independent Reviewer to Consider Special Law Enforcement Surveillance Powers' (Media Release, 19 July 2024).

13 *INSLM Act* s 6(1E)(a).

14 *INSLM Act* s 8.

15 *Intelligence Services Act 2001* (Cth) s 29(1)(bcaa) (*IS Act*).

16 *PJCIS SLAID Report* 131 [6.55].

enforcement arrangements (ACIC Review); and a Parliamentary Joint Committee on Law Enforcement (PJCLE) *Inquiry into the capability of law enforcement to respond to cybercrime* (PJCLE Cybercrime Review).

Comprehensive review and electronic surveillance reform

1.10 The *Report of the Comprehensive Review of the Legal Framework of the National Intelligence Community* (2019 Comprehensive Review) recommended that legislation governing the use of telecommunications interception, computer access and surveillance devices powers, including the *Surveillance Devices Act 2004* (Cth) (*SD Act*), be repealed and replaced with a new Act.[17] The government accepted this recommendation in December 2020.[18]

1.11 In line with that recommendation, the Department of Home Affairs (Home Affairs) commenced a major electronic surveillance reform (ESR) project, which was later transitioned to the Attorney-General's Department (AGD). In a recent machinery of government change, responsibility for the ESR project was moved back to Home Affairs.[19] I had a number of productive meetings with departmental officials from the ESR team during this review. The ESR project was initially conceived as a 2-year project, with a Bill to be finalised in 2023. However, the project is ongoing.[20] In evidence to this INSLM review in February 2025, AGD said that, given the complexity of the legislation and volume of technical issues, it has taken an 'extended period to work through many of the policy issues.' At that time AGD hoped to be able to progress further consultation on the ESR project shortly.[21]

1.12 The *SLAID Act* was introduced and enacted after the ESR project commenced. There has been no amendment to modify the requirement that I review the *SLAID Act* in the intervening years. Therefore, I have commenced this review in accordance with the statutory requirement of the *INSLM Act*, regardless of its timing relative to other potential electronic surveillance reforms that may arise from the ESR project.

17 Dennis Richardson, *Report of the Comprehensive Review of the Legal Framework of the National Intelligence Community* (Final Report, December 2019) vol 2, 268 Recommendation 75 (*2019 Comprehensive Review*).

18 Australian Government, *Commonwealth Government Response to the Comprehensive Review of the Legal Framework of the National Intelligence Community* (Government Response, December 2020) 23 (*Government response to the 2019 Comprehensive Review*).

19 Governor-General of the Commonwealth of Australia, *Administrative Arrangements Order* (13 May 2025).

20 Point in time web page accessible at Trove, 'Electronic Surveillance Reform', *Department of Home Affairs* (Web Page, 16 August 2022).

21 Sarah Chidgey, Deputy Secretary, Attorney-General's Department (AGD), *Public hearing transcript*, 20 February 2025, 79.

1.13 In its written submission to the present review, AGD stated that, in its view, a range of the matters that the Monitor is required to review and report on 'would be appropriately considered as part of the electronic surveillance reform, ensuring a consistent approach for all electronic surveillance powers.'[22] As discussed later in this report, some of the amendments this review recommends should be progressed without waiting for the ESR to be completed; others may be better implemented as part of holistic reforms.

ACIC Review

1.14 AGD published the unclassified report of the ACIC Review, and government response, on 14 November 2024. The independent reviewers 'reached the conclusion that comprehensive reform of the ACIC and the [*Australian Crime Commission Act 2002* (Cth)] is required to ensure the ACIC can be better positioned as Australia's national criminal intelligence agency.'[23] The ACIC Review found that ACIC's role and purposes had become unclear, noting the overlap between its functioning 'as either an intelligence agency or a law enforcement agency depending on the background and preference of the leadership of the day.' It considered ACIC would bring most value if it had a clear criminal intelligence function.[24] To that end, there were 29 recommendations made, 27 of which the government agreed to or agreed to in principle.[25]

1.15 Currently, ACIC is empowered to use each of the *SLAID Act* powers in the performance of its functions. Implementation of the ACIC Review recommendations is likely to affect the necessity and proportionality of the *SLAID Act* powers as they relate to ACIC. Therefore, when conducting this review I have been mindful of the ACIC Review findings.

PJCLE Cybercrime Review

1.16 On 16 October 2023, the PJCLE initiated an inquiry into the capability of law enforcement to respond to cybercrime. As noted in some submissions to the PJCLE, *SLAID Act* powers are among the tools that AFP and ACIC may use to respond to cybercrime.[26] I have had regard to evidence given to the PJCLE Cybercrime Review, particularly on the current threat of cybercrime and the challenges that law enforcement agencies face in responding to it. This PJCLE inquiry lapsed at the dissolution of the House of Representatives on 28 March 2025.

22 AGD, *Submission 20*, 9.

23 Stephen Merchant and Greg Wilson, *Independent Review of the Australian Criminal Intelligence Commission and Associated Commonwealth Law Enforcement Arrangements* (Report, May 2024) 7 (*ACIC Review*).

24 *ACIC Review* 17–18.

25 Australian Government, *Government Response to the Independent Review of the Australian Criminal Intelligence Commission and Associated Commonwealth Law Enforcement Arrangements* (Government Response, November 2024) (*Government Response to the ACIC Review*).

26 Cyber Security Cooperative Research Centre, Submission No 4 to PJCLE, Parliament of Australia, *Inquiry into the Capability of Law Enforcement to Respond to Cybercrime* (13 December 2023) 10; AFP, Submission No 22 to PJCLE, Parliament of Australia, *Inquiry into the Capability of Law Enforcement to Respond to Cybercrime* (January 2024) 9 [66], 25 [196].

Chapter 2: Overview of SLAID Act powers

2.1 The primary effect of the *SLAID Act* was the creation of 3 new warrants that AFP and ACIC may use:

- 2 new warrants in the *SD Act*:
  - the **data disruption warrant** (DDW), which enables AFP and ACIC to disrupt data by modifying, adding, copying or deleting it to frustrate the commission of relevant offences online
  - the **network activity warrant** (NAW), which allows AFP and ACIC to collect intelligence that relates to a 'criminal network of individuals' or anyone electronically connected to that group if it is relevant to the prevention, detection or frustration of one or more kinds of relevant offences
- one new warrant in the *Crimes Act 1914* (Cth) (*Crimes Act*):
  - the **account takeover warrant** (ATW), which allows AFP and ACIC to take control of a person's online accounts to gather evidence to further a criminal investigation into relevant offences.

2.2 Related powers for **assistance orders** and **emergency authorisation** were also introduced.

2.3 These warrants can be used covertly, often involve the use of advanced technology, can affect many people and – for NAWs in particular – can collect a lot of information, and for all of the warrants the chance of judicial review is remote. Despite this, the system for issuing warrants is almost the same as it was a century ago, when it was enacted for physical search warrants that allowed overt (and thus challengeable) searches of property to seize paper documents and other items. Understanding the history and recognising assumptions about the scope, technological simplicity and mechanisms to challenge early warrants goes some way to explaining why the current system for issuing warrants may be inadequate. This theme is introduced in this chapter and discussed further in Part 3 of this report.

Disruption powers – data disruption warrants

2.4 DDWs are a unique power. A DDW is not a step on the way to exercising a surveillance power; disruption is the goal.

2.5 There are limits to the kind of damage that can be caused under a DDW. DDWs must not be executed in a way that causes a person to be *permanently* deprived of money, digital currency or property that is not data. But, clearly, they can cause

loss of data and at least temporary deprivation of money or other property.[27] This 'disruption as objective' feature distinguishes DDWs from electronic surveillance warrants.

> Data disruption warrants are not properly categorised as an electronic surveillance power.

2.6 The strategy of police taking *otherwise lawful* actions to frustrate or disrupt crime before an offence is committed is uncontroversial – it plays an important role in reducing the harm the community suffers as a result of crime.[28] Examples include having a visible police presence in high crime areas, arresting a person (on the basis of appropriate evidence) for a lesser offence to stop the person from committing a more serious offence, and making those suspected of planning offences aware of police interest in their activities.

2.7 In contrast, DDWs allow AFP and ACIC to undertake disruption that would *otherwise be unlawful* if the warrant were sought based on a 'reasonable suspicion' of criminal activity. Unlike surveillance or search warrants, the main purpose is disruption, not collection of evidence for later prosecution and judicial decision. The Law Council of Australia has said that this means DDWs allow law enforcement officers to make 'conclusive assessments of criminality' and act as the 'judge, jury and executioner,' contrary to the key principle that only courts are to determine criminal guilt.[29]

2.8 The closest analogy is probably the *Proceeds of Crime Act 2002* (Cth), which allows for civil action to be taken to restrain and recover assets that are suspected to be of criminal origins, even where there has been no criminal conviction or the criminal burden of 'beyond reasonable doubt' has not been met.[30] Unlike DDWs, the Proceeds of Crime scheme requires judicial oversight and court orders must be sought before various actions can occur.

2.9 Another distinguishing feature of DDWs is that, unlike most other actions that may have a disruptive effect (such as execution of a search warrant, arrest on other charges or proceeds of crime actions), DDWs can be executed *covertly* and in circumstances where there is no real prospect of the matter ever coming before a

27 *SD Act* ss 27KE(7), 27KE(12).

28 See Attorney-General (Cth), *Ministerial Direction (Australian Federal Police): Australian Federal Police Act 1979, 20 October 2023*, 1–2; AFP Commissioner, *Commissioner's Statement of Intent* (20 October 2023) 1; AFP, *AFP Blue Paper To 2030 and Beyond: The Future of Federal Policing* (Paper, 16 July 2023) 10–11; Australian Criminal Intelligence Commission (ACIC), *Annual Report 2022–23* (Report, 18 October 2023) 36; David Bright and Chad Whelan, *Organised Crime and Law Enforcement: A Network Perspective* (Routledge, 2020) 110–27; Michael Skidmore, 'Lifting the Lid on "Disruption" as an Approach to Controlling Serious and Organised Crime' (Research Paper No 9, The Police Foundation, April 2023) 2–4.

29 Law Council of Australia (Law Council), Submission No 21 to PJCIS, Parliament of Australia, *Review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (9 March 2021) 32 [19]. See also *2019 Comprehensive Review* vol 3, 220–221 [38.70]–[38.73].

30 *Proceeds of Crime Act 2002* (Cth).

court.[31] This makes it very difficult for a person affected by a DDW to know that the disruption has taken place under a warrant and to take any action to challenge that warrant.

> DDWs can be executed covertly and in circumstances where there is no real prospect of the matter ever coming before a court.

2.10 Appropriately, other Australian government agencies, including the Australian Security Intelligence Organisation (ASIO), do not have proceeds of crime or data disruption powers. The Australian Signals Directorate (ASD) has a specific function 'to prevent and disrupt, by electronic or similar means, cybercrime undertaken by people or organisations outside Australia.'[32] The important difference between that function and DDWs is that foreign intelligence agency powers and functions must be directed at computers *outside* Australia. ASD does not have authority to disrupt computers inside Australia. Action by AFP and ACIC under DDWs can affect computers and data inside Australia.[33]

Identify powers – network activity warrants

2.11 NAWs allow AFP and ACIC to access data in multiple computers, where doing so is likely to 'substantially assist' in the collection of intelligence about a 'criminal network of individuals' and which is relevant to the prevention, detection or frustration of one or more 'relevant offences.'[34] This is a much lower threshold than that required to enliven other search and electronic surveillance powers and allows for surveillance of a very large number of computers under a single warrant.

2.12 When the Parliament was considering the SLAID Bill, AFP told the PJCIS that, without the type of 'technical and targeted intelligence power' they believed NAWs would provide, AFP's ability to obtain the information required to exercise overt law enforcement activities would be 'substantially diminished.' This was because traditional methods of intelligence and evidence gathering did not translate to an online environment where 'all participants and transactions are anonymised and communications are heavily encrypted.'[35] The NAW is intended to fill this gap by allowing collection of intelligence on a group of people for a law enforcement purpose. NAWs are specifically intended to be used for the collection of initial criminal intelligence to enable the subsequent targeted use of other statutory

31 The Revised Explanatory Memorandum makes clear that data disruption warrants are intended to 'offer an alternative action to AFP and ACIC, where the usual circumstances of investigation leading to prosecution are not necessarily the option guaranteeing the most effective outcome': Revised Explanatory Memorandum 3 [9]–[10].

32 *IS Act* s 7(1)(c).

33 For discussion on the importance of maintaining the distinction between foreign and security intelligence functions, see *2019 Comprehensive Review* vol 1, 195–199 [8.133]–[8.154].

34 *SD Act* s 27KK. For discussion of 'relevant offences,' see Chapter 10.

35 AFP, Submission No 6 to PJCIS, Parliament of Australia, *Review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (February 2021) 12 [55].

powers to gather evidence.[36]

> NAWs allow for surveillance of a very large number of people on the basis of a single warrant.

2.13 The targets of a NAW are computers used (or likely to be used) by individuals within a group that is a (somewhat misleadingly titled) 'criminal network of individuals.'[37] A 'criminal network of individuals' is defined as a group of people who are 'electronically linked,' where at least one member of the group uses an 'electronic service' or 'electronic communication' to engage in, facilitate or communicate about a 'relevant offence.'[38] AFP and ACIC can apply for a NAW even where it cannot ascertain the identities and location of the individuals or the specific target computers in the 'criminal network' and even though there may be changes over time to the composition of that network.[39] Further, there is no requirement for all or most of the individuals in the group to be engaged in or even know about the offending conduct. The breadth of this definition, and the impact of that breadth in the context of the NAW issuing framework, is discussed, alongside related terms such as 'computer' and 'relevant offence', in Chapter 10.

2.14 While other warrants with a relatively low threshold can authorise the collection of intelligence, these relate to national security, not law enforcement. For example, ASIO may apply to the Attorney-General for warrants authorising collection of security intelligence and foreign intelligence.[40] NAWs are the first law enforcement warrant to allow collection of intelligence with a threshold lower than the traditional 'reasonable suspicion' that the targeted person is engaged in criminal activity. A key safeguard is that intelligence gathered under a NAW cannot generally be used as evidence in a criminal prosecution. This also means that it is very unlikely a NAW would ever be subject to judicial review.

Takeover powers – account takeover warrants

2.15 An ATW authorises AFP or ACIC to 'take control' of one or more online accounts.[41] A person 'takes control' of an online account if they take one or more steps that result in that person having exclusive access to the account. This may include using an account's existing credentials to alter one or more account credentials, removing a requirement for 2-factor authentication or altering the kind or kinds of account

36 Revised Explanatory Memorandum 4–5 [19].
37 *SD Act* s 27KK. See Chapter 10 for a discussion of 'criminal network of individuals' and why this is a misleading expression.
38 *SD Act* s 7A.
39 *SD Act* s 27KK(2).
40 *Australian Security Intelligence Organisation Act 1979* (Cth) pt III div 2 (*ASIO Act*); *Telecommunications (Interception and Access) Act 1979* (Cth) pt 2-2 (*TIA Act*).
41 *Crimes Act* s 3ZZUR.

credentials required to access or operate the account.[42] They can be used overtly or covertly.

2.16 AFP or ACIC may apply for an ATW where there is a reasonable suspicion that one or more relevant offences has been, is being or is likely to be committed, an investigation into those offences is, will be, or is likely to be conducted, and taking control of the online account is necessary to enable evidence of those offences to be obtained.[43] AFP described the ATW as addressing situations where 'it is not operationally viable to seek the person's consent' to take over their account.[44]

2.17 The Revised Explanatory Memorandum explains that an ATW 'is designed to support existing powers, such as computer access and controlled operations,' with separate warrants or authorisations to be sought to use those existing powers.[45] In this sense, the ATW is not itself an electronic surveillance warrant. Instead, it has the functional effect of excluding a person from accessing their account for a period of time and enabling AFP or ACIC to access the account for that period. Agencies may only exploit that access for other purposes when permitted to do so by some separate, further authorisation. As AFP noted, the act of excluding a person from their account, without requiring further authorisation, may be a form of disruption by 'preventing access to illegal content that may be contained in the online account.'[46]

ATWs give clear authority for police to take control of an online account to secure evidence. But ATWs are not themselves used to conduct electronic surveillance.

Comparable Five Eyes law enforcement powers

2.18 I am unaware of any powers available to law enforcement agencies in a Five Eyes country that have the same explicit purposes as DDWs, NAWs or ATWs.

2.19 In the United Kingdom, certain agencies may utilise powers that are not explicitly for purposes equivalent to *SLAID Act* warrants to achieve a similar effect to a DDW in some circumstances. I understand that this may be done by one or a combination of a targeted equipment interference warrant and a property interference authorisation (and, depending on how a disruption activity is executed,

42 *Crimes Act* s 3ZZUL.
43 *Crimes Act* s 3ZZUN(1). See Chapter 10 for discussion for 'relevant offence.'
44 Ian McCartney, Deputy Commissioner, AFP, *Public hearing transcript*, 20 February 2025, 22. See also AFP, Submission No 6.1 to PJCIS, *Review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (April 2021) 5 [19]–[22].
45 Revised Explanatory Memorandum 6 [29].
46 AFP, *Submission 18*, 6 [35].

a targeted interception warrant).[47] The process for issuing these warrants in the United Kingdom is quite different from the current Australian system. In the United Kingdom, warrants must be approved by an independent judicial commissioner who is supported by independent technical advice, feedback from oversight inspections and advice from in-house counsel at the independent Investigatory Powers Commissioner's Office.[48]

Related SLAID Act powers

2.20 The *SD Act* and *Crimes Act* provide that certain senior AFP or ACIC officers can give an emergency authorisation to disrupt data or take over an account. This may be done only where there is an *imminent risk* of serious violence or substantial property damage and the circumstances are so serious that the disruption or takeover is *immediately necessary*.[49]

2.21 The circumstances must be so serious and of such urgency that disruption or takeover is warranted, and it must be impracticable in the circumstances to apply for a DDW or ATW, including an urgent warrant sought over the phone and without an affidavit. In addition, for an emergency authority for disruption of data, it must be established that there are no alternative methods of reducing or avoiding the risk that could have been used and would be likely to be as effective as data disruption.[50]

2.22 The *SD Act* and *Crimes Act* also provide for assistance orders to be issued in support of each of the 3 types of warrants. Assistance orders require a person specified in the order to provide any information or assistance that is reasonably necessary to allow AFP or ACIC to disrupt data, access data or take control of an online account.[51] Noncompliance with an assistance order can lead to imprisonment for up to 10 years.[52] Emergency authorisations and assistance orders are discussed in Part 5.

Where did the current arrangements for issuing warrants come from?

2.23 Before looking in detail at the current system for issuing warrants, it is useful to outline the origin of that system. To understand why the current system may be inadequate, it may be helpful to discuss the history of and the assumptions about the scope, technological simplicity and mechanisms that were in place to challenge early warrants.

47 Email from Investigatory Powers Commissioner's Office (IPCO) to INSLM, 25 July 2025. See *Police Act 1997* (UK) pt 3; Investigatory Powers Act 2016 (UK) pts 2, 5.
48 *Investigatory Powers Act 2016* (UK) pt 8 ch 1; IPCO, 'Authorisations' (Web Page).
49 *Crimes Act* ss 3ZZUX(1)(a)–(b); *SD Act* s 28(1C)(a)–(b).
50 *SD Act* s 28(1C)(ba).
51 *Crimes Act* s 3ZZVG; *SD Act* ss 64A, 64B.
52 *Crimes Act* s 3ZZVG(3); *SD Act* ss 64A(8), 64B(3).

2.24 Over 100 years ago the original *Crimes Act* made provision for a justice of the peace (and later a magistrate) to authorise search warrants that would apply to property.[53] The basic features of the system remain the same: a sworn affidavit from a constable and a decision against statutory criteria.[54] Because the original search warrants were for overt physical searches, there was an opportunity for an affected party to challenge the validity of the warrant and the admissibility of evidence. Even when the *Crimes Act* was amended to extend physical search warrants to the search of computers located on the searched premises,[55] the searches remained overt and thus open to challenge.[56]

2.25 When police got authority to intercept 'telephonic communications,' these were covert, but the system for issuing warrants was much the same: an affidavit, a judge and a reasonable possibility of material being challenged in evidence.[57] Although those warrants involved more technology than a physical search of premises, the technology involved in early 'wiretapping' is rudimentary in today's context and the volume of data available from intercepting a phone call in the late 1970's was far less than collection of internet communications and data today. The same is true for early state and territory surveillance devices and the Commonwealth ones that followed.[58] Computer access warrants for law enforcement agencies were added to the *SD Act* in 2018, and there was no comprehensive review of the warrant issuing system then or when *SLAID Act* warrants were introduced.[59]

> The basic process for issuing warrants has changed little in over 100 years. It is premised on overt warrants that do not involve complex technology, affect a very limited number of people, and collect limited information.

53 *Crimes Act* s 10, as enacted. That system substantially replicated even older arrangements in states and territories that were inherited from the United Kingdom.

54 *George v Rockett* (1990) 170 CLR 104, 113–14, citing *Caudle v Seymour* (1841) 1 QB 889, 893, 894. In *R v Tillett; Newton, Ex parte* (1969) 14 FLR 101, 108, Fox J said that s 10 of the *Crimes Act*, as enacted, conferred on a justice of the peace 'a grave and extraordinary power.'

55 *Crimes (Search Warrants and Powers of Arrest) Amendment Act 1994* (Cth) permitted use of electronic equipment at premises to see whether evidential material is accessible.

56 Delayed notification search warrants have been available for terrorism offences since 2014. Notice must be provided at a later date (usually within 6 months): *Crimes Act* pt IAAA.

57 AFP gained the ability to lawfully intercept telecommunications as a result of the *Telecommunications (Interception) Amendment Act 1979* (Cth). This was first extended to other police forces by the *Telecommunications (Interception) Amendment Act 1987* (Cth).

58 See, for example, *Listening Devices Act (No 69) 1984* (NSW) ss 15, 16(1), as enacted.

59 In PJCIS, *Review of the Amendments Made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Report, December 2021), the PJCIS recommended the government give further consideration to former INSLM James Renwick's proposal to establish an Investigatory Powers Division in the Administrative Appeals Tribunal (AAT) to realise a more robust authorisation process for certain powers exercised under the provisions of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (*TOLA Act*): Recommendations 20 and 21.

2.26 The only major change has been who issues warrants and in what capacity. The decision to expand the range of issuing authorities to include administrative tribunal members was made in light of the High Court's decisions in *Hilton v Wells*[60] and *Grollo v Palmer*,[61] which held that judges exercising federal judicial power may only be conferred non-judicial functions such as warrant issuing in a *personal capacity*.[62]

What is different about warrants today?

2.27 Arguably, the early system for issuing warrants was credible and effective at the time because searches were overt, so an affected person would be more likely to know about and could challenge the warrant. Furthermore, while the judge or magistrate needed to make a proper assessment of the application against set criteria, the execution of the warrants did not involve complicated technology.

2.28 *SLAID Act* warrants are technically complex and generally covert. The chance of an effective challenge to this type of warrant is remote, especially for DDWs and NAWs. A range of modern warrants, including NAWs, can potentially affect a very large number of people and can authorise the collection of volumes of data that were unimaginable at the time the original system for warrant issuing was developed. ATWs, and even more so DDWs, authorise interference with rights beyond surveillance or search and seizure of evidential material. These differences cast real doubt on the suitability of a warrant issuing system designed for an earlier time and less invasive warrants.

60 (1985) 157 CLR 57.
61 (1995) 184 CLR 348, 364–5 (Brennan CJ; Deane, Dawson and Toohey JJ).
62 AGD, *Submission 20*, 8–9, citing *Hilton v Wells* (1985) 157 CLR 57; and *Grollo v Palmer* (1995) 184 CLR 348.

Chapter 3: The threat of cybercrime

3.1 Each of the *SLAID Act* warrants is inherently cyber-related: DDWs and NAWs target data on computers; and ATW target accounts on online services. The explanatory materials reinforce that the warrants were introduced to assist police in addressing crime conducted or facilitated online. Therefore, I was mindful of the cyber threat environment in which the powers are to be utilised when considering the operation, effectiveness and proportionality of the warrants and associated powers. This chapter summarises evidence on the current threat of cybercrime to Australia and Australians; and the challenges that law enforcement and criminal intelligence agencies face in combating that threat.

What is 'cybercrime'?

3.2 The National Plan to Combat Cybercrime 2022 explains that there are 2 categories of crimes that fall within the concept of 'cybercrime':

> **Cyber-dependent** crimes directed at computers or other information communications technologies (ICTs) (such as computer intrusions and denial of service attacks) … [which] did not exist prior to the introduction of computers [and]
>
> **Cyber-enabled** crimes (such as online fraud, identity crimes and child sexual exploitation and abuse), which can increase in their scale and/or reach through the use of computers.[63]

3.3 Where the term 'cybercrime' is used in this report, it refers to both cyber-dependent and cyber-enabled crime. Examples of cyber-dependent crime include business email compromise; malicious software, including remote access trojans, keyloggers, viruses and worms; ransomware extortion; remote access scams; botnets; and phishing.[64]

3.4 Cyber-enabled crime refers to 'physical' crimes, such as drug trafficking, that are facilitated by electronic means, including encrypted devices and anonymising technologies. AFP has been involved in at least 2 well-publicised major operations targeting crimes planned or facilitated using Dedicated Encrypted Communication Devices:[65] Operation Ironside and Operation Kraken. Both operations led to the collection of a significant amount of evidence and the dismantling of dedicated encrypted communications platforms (the An0m app and Ghost) used exclusively

63 Australian Government, 'National Plan to Combat Cybercrime 2022' (Paper, 21 March 2022) 4. There can be overlap and co-dependency between cyber-dependent and cyber-enabled crimes – for example, the use of malware (involving unauthorised impairment of data, a cyber-dependent crime) to facilitate a scam (ie fraud, a cyber-enabled crime).

64 AFP, Submission No 22 to PJCLE, Parliament of Australia, *Inquiry into the Capability of Law Enforcement to Respond to Cybercrime* (January 2024) 3 [15].

65 A 'dedicated encrypted communication device' is a type of mobile electronic device that has been specifically modified with hardware and/or software to enable encrypted communication with other similarly modified devices.

for criminal purposes.[66] Operation Ironside occurred before *SLAID Act* warrants were introduced.

Current cybercrime threat

3.5 ASD warns:

> cybercrime is a persistent and disruptive threat. Cybercriminals are adapting to capitalise on new opportunities, such as artificial intelligence, which reduces the level of sophistication needed for cybercriminals to operate.[67]

In 2023–24, ASD received more than 87,400 reports of cybercrime with an average self-reported cost of $30,700 for individuals and between $49,600 and $63,600 for businesses.[68]

3.6 Collectively, the cost of cyber-dependent crime to individuals alone has been estimated at around $3.5 billion annually.[69] Of this, between $1.48 billion and $2.55 billion is attributed to serious and organised crime.[70] The total cost of cybercrime, including cyber-enabled crime, is more difficult to measure but is likely to be much higher.[71] Beyond the direct financial costs, cybercrime can also have a profound impact on the lives of victims, often including trauma and hardship.[72]

3.7 In its submission to this review, ACIC highlighted research showing that transnational, serious and organised crime (TSOC) cost Australia up to $68.7 billion

66 See AFP, 'Operation Ironside Third Anniversary: Offenders Jailed For a Collective 307 Years' (Media Release, 27 June 2024); AFP, 'AFP Operation Kraken Charges Alleged Head of Global Organised Crime App' (Media Release, 18 September 2024). Mentioning these operations here should not be taken to imply that they used *SLAID Act* warrants.

67 Australian Signals Directorate (ASD), *Annual Cyber Threat Report 2023–24* (Report, 20 November 2024) 1.

68 ASD, *Annual Cyber Threat Report 2023-24* (Report, 20 November 2024) 3.

69 Isabella Voce and Anthony Morgan, *Cybercrime in Australia 2023* (Statistical Report No 43, Australian Institute of Criminology, 2023) 8; citing Coen Teunissen, Isabella Voce and Russell Smith, *Estimating the Cost of Pure Cybercrime to Australian Individuals* (Statistical Bulletin No 34, Australian Institute of Criminology, 13 July 2021).

70 Russell Smith, *Estimating the Costs of Serious and Organised Crime in Australia, 2022–23* (Statistical Report No 50, Australian Institute of Criminology, 19 December 2024) 31–2.

71 In 2018, a study commissioned by Microsoft estimated that the 'potential' direct economic loss of cybersecurity incidents on Australian businesses was up to $29 billion, including tangible losses in revenue, decreased profitability and fines, lawsuits and remediation: Microsoft, 'Direct Costs Associated with Cybersecurity Incidents Costs Australian Businesses $29 Billion Per Annum' (Web Page, 26 June 2018). In 2021, ASD reported that there had been more than $33 billion in self-reported financial losses from cybercrime (including cyber-enabled crime) during 2020–21: Australian Cyber Security Centre (ACSC), *ACSC Annual Cyber Threat Report 1 July 2020 to 30 June 2021* (Report, 2021) 17. ASD noted these self-reported figures 'these figures may not be fully verified by law enforcement and a significant portion are related to cyber-enabled crimes.'

72 Isabella Voce and Anthony Morgan, *Cybercrime in Australia 2023* (Statistical Report No 43, Australian Institute of Criminology, 2023) 79–84.

in 2022–23, equating to 2.9% of Australia's gross domestic product.[73] It added that digital communications are 'critical' to TSOC actors, as they 'support the organisation, planning and logistics required to undertake criminal ventures as well as the passage of illicit funds generated from these activities.'[74]

3.8 The PJCLE Cybercrime Review also received significant evidence about the prevalence and threat of cybercrime. AFP submitted that the 'cybercrime ecosystem is continually evolving, enabling cyber criminals to consistently adapt while maintaining resilience to disruption efforts by law enforcement.'[75] It added that threats targeting critical infrastructure, governments, industry and the community are 'increasingly persistent and pervasive.'[76]

3.9 Other submitters to the PJCLE Cybercrime Review warned that official and media reporting 'vastly' underestimates the scale of victimisation and resulting losses.[77] The Cyber Security Cooperative Research Centre highlighted the diverse motivations behind cyber-criminal activity, with actors ranging from individuals and groups to state-sponsored actors and nation states.[78] Deakin University's Centre for Cyber Resilience and Trust submitted that the volume and complexity of cybercrime can be expected to only accelerate due to increasing geopolitical instability and the inability, or unwillingness, of some states to deal with cybercriminals operating within their borders.[79]

Cybercrime is a significant and growing issue.

73 ACIC, *Submission 17*, 2 citing Russell Smith, *Estimating the costs of serious and organised crime in Australia, 2022–23* (Statistical Report No 50, Australian Institute of Criminology, 19 December 2024).

74 ACIC, *Submission 17*, 2.

75 AFP, Submission No 22 to PJCLE, Parliament of Australia, *Inquiry into the Capability of Law Enforcement to Respond to Cybercrime* (January 2024) 3 [20].

76 AFP, Submission No 22 to PJCLE, Parliament of Australia, *Inquiry into the capability of law enforcement to respond to cybercrime* (January 2024) 5 [33].

77 IFW Global Investigations Pty Ltd, Submission No 36 to PJCLE, Parliament of Australia, *Inquiry into the Capability of Law Enforcement to Respond to Cybercrime* (February 2024) 11. See also Australian Institute of Criminology, Submission No 3 to PJCLE, Parliament of Australia, *Inquiry into the Capability of Law Enforcement to Respond to Cybercrime* (December 2023) 13; Cyber Security Cooperative Research Centre, Submission No 4 to PJCLE, Parliament of Australia, *Inquiry into the Capability of Law Enforcement to Respond to Cybercrime* (13 December 2023) 7.

78 Cyber Security Cooperative Research Centre, Submission No 4 to PJCLE, Parliament of Australia, *Inquiry into the Capability of Law Enforcement to Respond to Cybercrime* (December 2023) 5.

79 Centre for Cyber Resilience and Trust, Deakin Uni, Submission No 7 to PJCLE, Parliament of Australia, *Inquiry into the Capability of Law Enforcement to Respond to Cybercrime* (December 2023) 4.

3.10 I have had regard to the evidence provided to the PJCLE Cybercrime Review as well as information in submissions to this review. In short, there is no reason to doubt that cybercrime is a significant and growing issue. To respond to it, a wide range of actions by government, industry and individuals are required. One part of the response needs to be that law enforcement and criminal intelligence agencies having the capability and legal powers to collect intelligence and evidence in a proportionate and appropriately oversighted way.

Challenges in combating cybercrime

3.11 Collection of evidence and intelligence about cybercrime is often not straightforward. According to the Australian Institute of Criminology submission to the PJCLE Cybercrime Review, cybercrime has several characteristics that are likely to affect law enforcement responses – for example:

- Cybercrime comprises an extremely broad range of crime types, each with different targets, risk factors, offender motivations and modus operandi, harms to victims and response requirements.
- The modus operandi of perpetrators of cybercrime is constantly evolving in response to both emerging opportunities and government and law enforcement actions to disrupt prominent forms of cybercrime.
- Cybercrime that targets individual computer users is most frequently a high-volume, low-yield crime, with the overall cost to Australian individuals 'likely to be enormous,' even though median losses per victim are relatively small.[80]

3.12 The challenges for law enforcement agencies in combating cybercrime was also described in evidence provided to this review. AFP highlighted encryption and anonymising technology, saying:

> The AFP's operating environment is increasingly complex and rapidly evolving. Over the last decade, the AFP has observed an exponential uptake in the use of end-to-end encryption and anonymising technology, including the dark web, to facilitate serious crime and national security threats.[81]

3.13 AFP provided evidence about how often encryption impedes traditional police surveillance:

> In 2022–23, 96.1 percent of the AFP's lawfully intercepted content was unintelligible due to encryption. This has had a significant impact on AFP investigations. [For example], between 2020 and 2023, encrypted WhatsApp messaging impeded over 400 AFP operations, with usage increasing by 270 per cent during this time.[82]

80 Australian Institute of Criminology, Submission No 3 to PJCLE, Parliament of Australia, *Inquiry into the Capability of Law Enforcement to Respond to Cybercrime* (December 2023) 4–7.
81 AFP, *Submission 18*, 2 [5].
82 AFP, *Submission 18*, 3 [15].

3.14 ACIC said it had faced similar challenges, noting that:

> the use of anonymised, sophisticated and encrypted technologies by TSOC entities to communicate securely, particularly [dedicated encryption communications devices] platforms, has degraded the effectiveness of traditional telecommunications interception and the ability to access communications content to support law enforcement and intelligence operations.[83]

3.15 ACIC said that organised criminal groups were utilising 'security hardening' features and 'cutting edge technology' to support unlawful activities:

> The current transnational serious and organised crime (TSOC) threat – overlaid by the contemporary digital communications environment – presents challenges to the ACIC … [TSOC actors] use encryption and security hardening features in conjunction with other cutting-edge technology – sometimes developed specifically by criminals exclusively to support unlawful activities – and both legitimate and 'grey' service providers to enhance their effectiveness, remain anonymous and evade identification and detection.[84]

3.16 AGD reiterated these points, saying, '[t]he threat environment has continued to develop with serious and organised crime groups readily adapting to, adopting and exploiting new technologies to their advantage.'[85]

There is evidence that encryption and other 'security hardening' features make it difficult to gather intelligence and evidence online.

3.17 The nature of online crime means that, especially for cyber-dependent crimes, there is no need for criminals to be physically inside Australia. Indeed, AFP has said that 'Australia's most significant cyber criminals and syndicates are based offshore.'[86] The challenges associated with disrupting data or access to accounts outside Australia are discussed further in Chapter 18.

83 ACIC, *Submission 17*, 2.
84 ACIC, *Submission 17*, 2.
85 AGD, *Submission 20*, 3.
86 AFP, Submission No 22 to PJCLE, Parliament of Australia, *Inquiry into the Capability of Law Enforcement to Respond to Cybercrime* (January 2024) 4 [31]. See also ASD, *ASD Cyber Threat Report 2022–23* (Report, 14 November 2023) 38.

Part 2. Use, effectiveness and ongoing necessity

SLAID Act powers have been used sparingly, and largely against the serious offences for which they were introduced. AFP and ACIC use of NAWs has led to the collection of intelligence about serious crimes that could not have been gathered using traditional surveillance warrants. AFP use of ATWs has enabled online accounts to be taken over so that evidence can be preserved and accessed using other powers. In some cases, AFP has used DDWs where regulatory powers, as well as prosecution and other traditional law enforcement techniques, would have been ineffective.

While additional safeguards are needed, especially in the way warrants are issued, I am satisfied that there is an ongoing need for AFP and ACIC to continue to have access to NAWs and ATWs and for AFP to have access to DDWs.

ACIC has not used any ATWs or DDWs. Nevertheless, there is a good case for ACIC retaining the ability to take over online accounts, although this should be for intelligence-gathering purposes in accordance with ACIC's role as a criminal intelligence agency. DDWs are an extraordinary power and are not an intelligence power, so their use should be restricted to only AFP.

The operational utility of ATWs could be improved by introducing 'named person ATWs.' I heard evidence that people engaged in serious criminal activity often use multiple online accounts. AFP said that, in some situations when executing warrants, it had identified additional, previously unknown accounts. Also, given some types of online accounts can be deleted quickly, there is currently a risk that evidence could be lost from accounts that were not included in the original ATW. This can be the case even when an issuing authority is satisfied that taking over the known accounts belonging to a person is necessary and proportionate.

NAWs can currently be issued for a maximum of 90 days but can be renewed any number of times. The 90-day limit does not recognise that intelligence operations supported by NAWs are often lengthy. The unlimited renewals mean that a report is often not provided to the Minister and oversight body for a very long time given that currently that type of reporting is only required once the warrant and any renewals have ceased to have effect. This is problematic for oversight and accountability. It should be possible to issue NAWs for up to 6 months and provide a full report to the Minister as soon as practicable after the 6 months, even if a further warrant is sought.

Chapter 4: Use and effectiveness of SLAID Act warrants

4.1 Fewer than 50 *SLAID Act* warrants (including extensions) were sought in the first 3 years of their operation. This shows that restraint is being exercised when using these significant powers. Also, practical limitations arise because of the complex technology and specialised skills required to execute some of the warrants.

4.2 The utility of *SLAID Act* warrants is not demonstrated in existing public reporting. The warrants have been effective in understanding criminal networks and combating serious crimes.

4.3 This chapter considers the overall use and effectiveness of *SLAID Act* powers with a focus on the 3 types of warrants. Part 5 of this report looks in more detail at the use and effectiveness of associated emergency authorisations and assistance orders.

Use of SLAID Act powers

4.4 The *SLAID Act* powers have been used sparingly. Between 4 September 2021 (when the *SLAID Act* commenced) and 31 December 2024, DDWs, NAWs and ATWs were issued a collective **26 times** (not including extensions). If extensions are included, that total increases to **47 times**. No urgent warrants were sought. One emergency authorisation for an ATW was given (and subsequently approved).[87]

4.5 The majority of warrants were issued to AFP. ACIC has not sought any ATWs or DDWs. In all but one case, warrants and renewals were granted in the first instance. In one case, the initial application was denied and further information sought. When that information was provided, the warrant was issued.

4.6 The number of *SLAID Act* warrants is set out in Tables 1 and 2 below, with data drawn from annual reports and statistics provided to the Monitor.[88] Figures cover the period 4 September 2021 to 31 December 2024.

87 AFP, *Annual Report 2023–24* (Report, 16 September 2024).

88 See AGD, *Surveillance Devices Act 2004 Annual Report 2021–22* (Report, November 2022) 26, 30 (*SD Act Annual Report 2021–22*); AGD, *Surveillance Devices Act 2004 Annual Report 2022–23* (Report, November 2023) 27, 31 (*SD Act Annual Report 2022–23*); AGD, *Surveillance Devices Act 2004 Annual Report 2023–24* (Report, November 2024) 27, 30 (*SD Act Annual Report 2023–24*); AFP, *Annual Report 2021–22* (Report, 12 September 2022) 168; AFP, *Annual Report 2022–23* (Report, 14 September 2023) 170; AFP, *Annual Report 2023–24* (Report, 16 September 2024) 150–1; ACIC, *2023–24 Account Takeover Warrant Annual Report* (Report, October 2024); ACIC, *Account Takeover Warrant Annual Report to Minister 1 July 2022 to 30 June 2023* (Report, August 2023); ACIC, *Crimes Act 1914 – Account Takeover Warrant Annual Report to Minister for the Period 4 September 2021 to 30 June 2022* (Report, February 2023).

Table 1 – AFP use of SLAID Act powers, 4 September 2021 to 31 December 2024

	2021–22	2022–23	2023–24	1 July 24 – 31 Dec 24
DDWs	2 warrants issued	Nil	1 warrant issued	2 warrants issued
NAWs	1 warrant issued 2 warrant extensions	1 warrant issued 5 warrant extensions	2 warrants issued 3 warrant extensions	Nil warrants issued 3 warrant extensions
ATWs	2 warrants issued	3 warrants issued	6 warrants issued	3 warrants issued

Note: The information for 1 July 2024 – 31 December 2024 is provisional and reflects information provided to the Monitor by AFP and ACIC before those statistics were finalised for the 2024–25 financial year.

Table 2 – ACIC use of SLAID Act powers, 4 September 2021 to 31 December 2024

	2021–22	2022–23	2023–24	1 July 24 – 31 Dec 24
DDWs	Nil	Nil	Nil	Nil
NAWs	1 warrant issued 1 warrant extension	2 warrants issued 1 warrant extension	Nil warrants issued 4 warrant extensions	Nil warrants issued 2 warrant extensions
ATWs	Nil	Nil	Nil	Nil

Note: The information for 1 July 2024 – 31 December 2024 is provisional and reflects information provided to the Monitor by AFP and ACIC before those statistics were finalised for the 2024–25 financial year.

Offences the warrants have been used for

4.7 *SLAID Act* warrants *can be* sought for a very broad range of offences – essentially any Commonwealth offence (or state offence with a federal aspect) that has a penalty of 3 years or more plus some additional specific offences.[89] The question of how broad the definition of 'relevant offence' *should* be is discussed in Chapter 10.

4.8 When the need for the new warrants was described, only a limited number of very serious offences were discussed. These included 'child abuse and exploitation, terrorism, the sale of illicit drugs, human trafficking, identity theft and fraud, assassinations, and the distribution of weapons.'[90]

4.9 The relevant offences that have been the subject of all 3 warrants have mostly been consistent with the limited set of very serious offences described in the Revised Explanatory Memorandum.[91] All warrants have referred to offences with a maximum penalty of 5 years or more, although some NAWs sought by ACIC have also included offences with a maximum penalty of 3 years.[92]

4.10 The focus on more serious offences is consistent with the remit of ACIC and AFP. For ACIC this is 'to collect, analyse and disseminate intelligence relevant to [transnational, serious and organised crime].'[93] AFP's functions are broader, but there is a ministerial direction requiring AFP 'to focus on the most serious levels of criminality and criminal offences.'[94]

4.11 The types of offences *SLAID Act* warrants have been used for are summarised in Table 3 below.[95]

89 See the definitions of 'relevant offence' in *SD Act* s 6 and *Crimes Act* s 3ZZUK.
90 Revised Explanatory Memorandum 2 [4].
91 See Revised Explanatory Memorandum 2 [4].
92 Wendy Darling, National Manager, ACIC, *Public hearing transcript*, 20 February 2025, 48.
93 Heather Cook, CEO, ACIC, *Public hearing transcript*, 20 February 2025, 46. See also the definition of 'relevant crime' in *Australian Crime Commission Act 2002* (Cth) s 4 (*ACC Act*).
94 Ian McCartney, Deputy Commissioner, AFP, *Public hearing transcript*, 20 February 2025, 29; see Attorney-General (Cth), *Ministerial Direction (Australian Federal Police): Australian Federal Police Act 1979*, 20 October 2023.
95 *SD Act Annual Report 2021–22* 25, 29; *SD Act Annual Report 2022–23* 26, 30; *SD Act Annual Report 2022–23* 26, 29; AFP, *Annual Report 2021–22* (Report, 12 September 2022) 168; AFP, *Annual Report 2022–23* (Report, 14 September 2023) 171; AFP, *Annual Report 2023–24* (Report, 16 September 2024) 151.

Table 3 – Offences for which SLAID Act warrants have been issued

DDWs	Dishonestly obtaining or dealing in personal financial information Unauthorised access, modification or impairment of data with intent to commit a serious offence Dealing in the proceeds of crime
NAWs	Serious drug offences Telecommunications offences Money laundering offences Criminal association and organisation offences Firearm offences Dealing with proceeds of crime Dangerous weapons offences Trafficking in person offences Child abuse material offences
ATWs	Using a carriage service for child abuse material Using a carriage service to make a threat to kill Using a carriage service to menace, harass or cause offence Conduct for the purposes of electronic service used for child abuse material Possessing or controlling child abuse material obtained or accessed using a carriage service Possessing, controlling, producing, supplying or obtaining child abuse material for use through a carriage service Urging violence against groups Advocating terrorism Intentional foreign interference Preparing for a foreign interference offence Other acts done in preparation for, or planning, terrorist acts Membership of a terrorist organisation Recruiting for a terrorist organisation Serious drug offences Using a carriage service for violent extremist material Possessing or controlling violent extremist material obtained or accessed using a carriage service Supporting a criminal organisation Dealing with proceeds of crime

Factors contributing to limited use

4.12 Evidence provided to this review indicates that both 'judicious use' and practical factors have contributed to the relatively small number of *SLAID Act* warrants being used. ACIC said:

> The ACIC is judicious in its application of all covert and intrusive powers and uses the least invasive and most effective and appropriate power depending on the particular circumstances of the operation it is conducting.[96]

4.13 Similarly, AFP said:

> The AFP is judicious about the use of these powers available to us, the direction of an investigation and the implications that may arise.[97]

4.14 The use of the *SLAID Act* powers has also been affected by practical limitations, including cost, resourcing and technological capability. When referring to the fact that it had not yet sought DDWs or ATWs, ACIC said:

> While preparing to operationalise the SLAID Act powers, the ACIC encountered environmental, research and development, and technical challenges. This has meant that operationalisation of the powers has taken significantly longer than originally anticipated and that benefits and outcomes of use of the full suite of powers is yet to be realised. It is as a direct result of the technical complexity, requirement for capability development and investment, and operational opportunities, as well as the need to ensure proportionate and appropriate use, that the ACIC is yet to apply for a data disruption warrant (DDW) and account takeover warrant (ATW).[98]

4.15 AFP also provided evidence about how the use of these warrants is limited to particular areas of the agency:

> because of the technical expertise and knowledge required, the execution of these warrants is restricted to specific commands with the necessary experience and skills to make informed decisions when executing SLAID powers.[99]

Significant technical expertise and capability are needed to fully utilise SLAID Act powers.

96 ACIC, *Submission 17*, 5.
97 Ian McCartney, Deputy Commissioner, AFP, *Public hearing transcript*, 20 February 2025, 22.
98 ACIC, *Submission 17*, 3.
99 Ian McCartney, Deputy Commissioner, AFP, *Public hearing transcript*, 20 February 2025, 22.

Effectiveness of powers

4.16 To assess the effectiveness of warrants, to a large extent this review relied on evidence from agencies. However, general assertions of effectiveness were not sufficient. The review sought specific examples from agencies at both public and private hearings and also examined reports made to ministers about warrants.

Claims of effectiveness in initial agency submissions

4.17 In their initial submissions to this review AFP, ACIC and AGD asserted that the *SLAID Act* warrants have been effective in combating serious criminal activity. AFP said that while their use of *SLAID Act* powers has not been extensive:

> the powers have been of significant benefit to the AFP's work in investigating, preventing and disrupting serious crime, including malware, phishing, cyber-enabled scams and fraud, importation of controlled substances, publishing and distribution of child exploitation materials and terrorism.[100]

4.18 ACIC said that 'the SLAID Act has enhanced the ACIC's ability to access and collect information on [transnational, serious and organised crime] networks, reaping significant benefits across the domestic and international law enforcement and intelligence community.'[101]

4.19 Based on the advice of AFP and ACIC, AGD said that the warrants have achieved their policy objective:

> The *SLAID Act* was designed to enhance the ability of the AFP and ACIC to discover, target, investigate and disrupt serious cyber-enabled crime, in particular, in the context of increasing use of anonymising technologies by serious and organised criminal actors. The powers have achieved this policy objective.[102]

4.20 I agree with Lord Anderson QC, who said, in the context of his 2015 review of bulk powers in the United Kingdom, that something more than mere assertions is required to substantiate claims of effectiveness:

> In approaching my task, I have proceeded on the basis … [that] … (a) I have not assumed that the powers under review have utility, even when expert security-cleared bodies have previously opined that this is the case. (b) On the contrary, I have required the Government … to make good from first principles their claims of utility.[103]

100 AFP, *Submission 18*, 4–5 [24].
101 ACIC, *Submission 17*, 2.
102 AGD, *Submission 20*, 4.
103 David Anderson, Independent Reviewer of Terrorism Legislation, *Report of the Bulk Powers Review* (Report, August 2016) 74–6 [4.11]–[4.24].

4.21 The general assertions and largely hypothetical examples in the initial submissions of the agencies did not provide sufficient evidence for me to be satisfied of the utility of the warrants. I therefore sought more information so I could assess this.

> General assertions and largely hypothetical examples did not provide sufficient evidence for me to be satisfied of the utility of the warrants.

Publicly available information does not support claimed utility

4.22 There is limited publicly available information about the use of *SLAID Act* warrants. Published statistics indicate that *SLAID Act* powers have resulted in one arrest, which in isolation does not provide a strong basis for claims about the effectiveness and utility of these powers.[104]

4.23 This view was shared by many non-government submitters. The Queensland Council for Civil Liberties was of the view that a result of one arrest from the *SLAID Act* powers 'cannot justify the necessity of these powers and we are left only with the assertions made by agencies.'[105] Dr Glover stated that 'a convincing Operational Case for the powers that is acceptable to an informed electorate has yet to be placed in the public domain.'[106] In a similar vein, Digital Rights Watch questioned the measure that agencies were using to calculate effectiveness.[107]

4.24 Current annual reporting requirements for *SLAID Act* powers (discussed in more detail in Chapter 15) are based on historical requirements for evidence collection warrants – they are not tailored to the quite different purposes of these powers.

4.25 In the case of ATWs, there is an express requirement to publicly report on arrests and prosecutions made based on information *obtained under* the warrants.[108] Given that the primary use of an ATW is to take control of an online account to obtain evidence through *other means*, it is likely that only very limited information will ever be obtained under the ATW itself. This means that current reporting does not properly reflect the extent to which an ATW has been a contributing factor to arrests and prosecutions.

104 AFP, *Annual Report 2023–24* (Report, 16 September 2024) 151. Statistics about prosecutions and arrests for data disruption warrants (DDWs) and network activity warrants (NAWs) provided to the Monitor by AFP showed there had been nil arrests or prosecutions in connection with those warrant types.
105 Queensland Council for Civil Liberties (QCCL), *Submission 6*, 5.
106 Philip Glover, *Submission 8*, 2–3.
107 Digital Rights Watch, *Submission 22*, 2.
108 *Crimes Act* ss 3ZZVM(1)(p)–(q); AFP, *Annual Report 2023–24* (Report, 16 September 2024) 150–1; ACIC, *2023–24 Account Takeover Warrant Annual Report* (Report, October 2024) 1–2.

4.26 The utility of current public reporting of the same information for DDWs and NAWs is also questionable. There is no express requirement to separately publish this type of information about DDWs and NAWs, and the information has not been separately reported in the annual reports published to date.[109] Even if the relevant statistics for DDWs and NAWs were separately reported, information on the number of arrests and prosecutions is likely to be of limited utility in increasing public confidence in the effectiveness of *SLAID Act* warrants. As recognised by AGD, DDWs and NAWs 'rarely directly result in arrests and prosecutions' given their focus on disruption of online criminal activity and intelligence collection respectively.[110] This is consistent with evidence given to me during this review that no arrests or prosecutions have been made, wholly or partly, based on information obtained under a DDW or NAW between 4 September 2021 and 31 December 2024. I was also advised that NAWs have contributed to intelligence about individuals who have later been arrested, but, as arrests are strictly based on admissible evidence, intelligence gathered under a NAW is not counted as leading to the arrest.[111]

> Reporting on arrests and prosecutions is of little utility in assessing the effectiveness of *SLAID Act* warrants.

4.27 The limitations of reporting on numbers of prosecutions and arrests as a means of assessing and reporting on the effectiveness of the *SLAID Act* powers is particularly acute for ACIC:

> As an intelligence organisation, as opposed to a law enforcement organisation … we don't measure our success by the number of prosecutions or arrests. We measure in terms of the value from the intelligence derived from these operations. And as an intelligence organisation, the most important thing is that we are discovering things that weren't previously known …[112]

4.28 I consider that more can be done to report publicly on the effectiveness of these warrants. This is discussed in Chapter 15.

Evidence on effectiveness provided at the public hearing

4.29 In their evidence at the public hearing, ACIC and AFP provided more detailed information about the benefits of their use of *SLAID Act* powers.

109 *SD Act Annual Report 2023–24* 32; *SD Act Annual Report 2022–23* 32; *SD Act Annual Report 2021–22* 31.
110 AGD, *Submission 20*, 26.
111 Email from AFP to INSLM, 4 April 2025.
112 Heather Cook, CEO, ACIC, *Public hearing transcript*, 20 February 2025, 43.

4.30 ACIC gave a specific example of how the use of a NAW led to the initial identification of a criminal syndicate that was not previously known to be operating in Australia:

> Network Activity Warrants have enabled the ACIC to identify and target high-threat criminal networks impacting Australia and to understand and identify critical points within those networks. Work under these warrants has delivered intelligence on high-level criminal actors, along with the identification of previously unidentified criminal syndicates engaged in serious activity.[113]

4.31 AFP, noting the limitations it faced in giving specific details in a public forum, stated:

> [We can use a DDW to] distribute at scale the ability to neutralise [the threat of cybercrime through the use of malicious software] across potentially tens of thousands of computers concurrently across Australia, which we couldn't practically do through other more traditional law enforcement means … We're talking about potentially tens of thousands of victims and millions of dollars in terms of preventative activity in the future.[114]

4.32 These examples were of more assistance than initial submissions and published statistics.

Evidence on effectiveness provided at private hearings

4.33 Evidence on how the warrants have been used was also sought at private hearings. Most of the details of the actual operations where the warrants have been or currently are being used cannot be published without risk to methodologies and current investigations. However, I can provide the following information about the additional examples discussed at private hearings:

- DDWs have been used for phishing and malware operations. This has helped to protect Australians from these sorts of activities.[115]
- AFP has used NAWs for intelligence gathering on serious and organised crime, including crimes involving drugs, firearms, money laundering and people trafficking.[116]
- NAWs enhanced ACIC's awareness of the environment that serious and organised crime networks operate within and the people they interact with. Information obtained from NAWs had informed other criminal intelligence activities.[117]
- AFP has used ATWs in parallel with other authorities, including search warrants and controlled operations authorities.[118]

113 Heather Cook, CEO, ACIC, *Public hearing transcript*, 20 February 2025, 42.
114 Rob Nelson, Commander, AFP, *Public hearing transcript*, 20 February 2025, 24–5.
115 INSLM, *Summary of private hearing – AFP*, 23 July 2024, 2.
116 INSLM, *Summary of private hearing – AFP*, 23 July 2024, 3.
117 INSLM, *Summary of private hearing – ACIC*, 29 July 2024, 2.
118 INSLM, *Summary of private hearing – AFP*, 23 July 2024, 3.

Ministerial reporting on effectiveness

4.34 Agencies are required to report to the Minister about each DDW and NAW, including details of the benefits of the warrant.[119] As part of this review, INSLM staff reviewed all reports available as at 11 February 2025.[120]

4.35 Many of the reports included detailed and compelling information about the effectiveness of the individual warrants for combatting serious crimes. For example, AFP reports described a significant number of instances of malware being disrupted with a DDW, information collected under a NAW providing indicators of criminal activity, methods and associates that could not be obtained by other mechanisms or was previously unknown, and the taking over of an account under an ATW preventing the deletion of evidence.

Findings on the effectiveness of SLAID Act warrants

4.36 My views on the effectiveness of warrants has been informed by evidence given at both public and private hearings and through the review of classified reports provided to ministers. Based on this information, I am satisfied that *SLAID Act* warrants have been effective in understanding criminal networks and combating serious crimes. Furthermore, they have been used in situations where other types of warrants would probably have been ineffective. The effectiveness of the current safeguards is a different matter and is discussed later in this report, see in particular Part 3 and Part 4.

SLAID Act warrants have been used to understand criminal networks and to combat serious crimes.

119 *SD Act* ss 49(1), 49(2D)–(2E). Account takeover warrants (ATWs) are not subject to individual reporting, only an annual report: *Crimes Act* ss 3ZZVL, 3ZZVM.

120 Copies of warrants and reports as at 11 February 2025 were produced by both AFP and ACIC in response to notices under s 24 of the *INSLM Act*. There were limited reports available on use of NAWs because the requirement to report at the conclusion of a warrant is not triggered if the NAW is extended, as is the case for most NAWs that have been issued (see Chapter 15).

Chapter 5: Ongoing necessity of SLAID Act powers

5.1 There is little doubt that Australia faces a significant and persistent threat from cybercrime. However, it does not automatically follow that this means it is necessary to retain the *SLAID Act* powers. To assess whether it is necessary to retain the powers, it is important to consider the threat, how the powers have been used and the existence of alternative mechanisms for addressing the threat.

5.2 This chapter looks at alternative mechanisms that are available. It concludes that some form of criminal intelligence, data disruption and account takeover powers would need to continue – subject to improvements to the current safeguards and in particular the system for issuing warrants. It then considers the related question of where those powers should reside given the different functions of AFP and ACIC. The conclusion is that ACIC should not have disruption powers, but it requires NAWs and an intelligence-focused account takeover power. AFP should retain intelligence, disruption and account takeover powers. The recommendation that any of these powers be retained is subject to improvements in the way warrants are issued and in strengthening other safeguards, which are discussed later in this report (see in particular Part 3 and Part 4).

Other mechanisms for combating cybercrime

5.3 The *SLAID Act* powers form part of a broad suite of Commonwealth laws relevant to the prevention, investigation, punishment and disruption of cybercrime. These include:

- **criminal offences** that concern cybercrime, including pt 10.6 (telecommunications offences), pt 10.7 (computer offences) and pt 10.8 (financial information offences) of the *Criminal Code Act 1995* (Cth) (*Criminal Code*)[121]
- **general law enforcement powers**, including search warrants under the *Crimes Act*, computer access warrants under the *SD Act*, and telecommunications interception powers under the *Telecommunications (Interception and Access) Act 1979* (Cth) (*TIA Act*), as well as laws that support cooperation with industry on the development and use of capabilities needed to exercise these powers such as the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (*TOLA Act*)

[121] As of 22 October 2024 AGD was undertaking a review of these offences to ensure that the framework is fit for purpose given the increasing and evolving threat posed by cybercriminal conduct online: Evidence to PJCLE, Parliament of Australia, Canberra, 22 October 2024, 33 (Parker Reeve); See also AGD, Submission No 12 to PJCLE, Parliament of Australia, *Inquiry into the capability of law enforcement to respond to cybercrime* (December 2023) 9.

- **laws that protect critical infrastructure**, such as infrastructure vulnerable to cyberattacks, including the *Security of Critical Infrastructure Act 2018* (Cth)
- **cybersecurity laws**, including the *Cyber Security Act 2024* (Cth), which introduced mandatory reporting obligations for businesses where ransomware payments are made and the setting of mandatory security standards for internet connected products
- the *Online Safety Act 2021* (Cth), which provides for **directions to be given to online service providers** to remove certain material (including certain illegal and restricted online material) or access to that material through the use of notices.[122] This extends to a range of material from the 'most seriously harmful material' (for example, videos of sexual abuse of children or which advocate terrorism) to 'material which is inappropriate for children' (for example, online pornography)[123]
- **laws requiring online service providers** to assist Commonwealth, state and territory officials, including to enforce the law and protect national security. This includes restricting access to online services and blocking websites[124]
- Australia's **autonomous sanctions regime** in relation to significant cyber incidents. This was recently used to impose financial sanctions and travel bans on individuals and a cybercriminal infrastructure provider for offering services that enabled criminal networks to facilitate unlawful activity[125]
- the powers and functions of the **ASD to prevent and disrupt**, by electronic or similar means, cybercrime undertaken by people or organisations **outside** Australia and to **provide advice and assistance** on information security.[126]

122 *Online Safety Act 2021* (Cth) pt 9, divs 1–6.

123 eSafety Commission, *Online Content Scheme: Regulatory Guidance* (Guide, January 2025) 3. The eSafety Commissioner's powers depends on there being a sufficient nexus to Australia: *eSafety Commissioner v X Corp* [2024] FCA 499.

124 See *Telecommunications Act 1997* (Cth) s 313; Department of Infrastructure, Transport, Regional Development, Communications and the Arts, *Guidelines for the Use of s 313(3) by Government Agencies for the Lawful Disruption of Access to Online Services* (Guideline, June 2017). See also Australian Communications and Media Authority and eSafety Commissioner, *Annual Report 2023–24* (Report, 26 September 2024) 99. In 2023–24, there were 142 requests and 7,783 online services blocked.

125 See, for example, Department of Foreign Affairs and Trade, 'Significant Cyber Sanctions Framework', *Sanctions Regimes* (Web Page); AFP, 'AFP Joins Global Crackdown on Cybercriminal Infrastructure Provider' (Media Release, 12 February 2025).

126 This does not allow ASD to disrupt computers inside Australia: *IS Act* ss 7(1)(c)–(ca), 7(e), 14.

5.4 There are also several Commonwealth regulatory agencies with responsibilities in cybercrime, including the Australian Competition and Consumer Commission (in particular, the National Anti-Scam Centre),[127] the Australian Communications and Media Authority[128] and the eSafety Commissioner.[129]

5.5 Some submissions to this review questioned the ongoing necessity of the *SLAID Act* powers given the wide range of other available mechanisms for combating cybercrime. The Australian Human Rights Commission said, 'it is also relevant that there are a range of other existing statutory mechanisms directed at combatting cybercrime and a lack of directly comparative powers in other Five Eyes countries.'[130] The Law Council of Australia submitted that this was particularly the case with DDWs and that the ongoing necessity of AFP having these powers 'should be reassessed in light of material changes to the resourcing of the ASD since 2022.' The Law Council of Australia also noted that the regulatory tools available to address cyber-dependent crime have been significantly enhanced since the passage of the *SLAID Act* in 2021.[131]

Findings on ongoing necessity of SLAID Act powers

5.6 In assessing the ongoing necessity of *SLAID Act* powers, I have considered the availability of other mechanisms and recognise that these mechanisms may be used as an alternative to *SLAID Act* powers in certain circumstances.

5.7 For example, one of the potential uses of a DDW provided in the Revised Explanatory Memorandum was to redirect a person away from a child exploitation website, thereby denying them access to child exploitation material.[132] In practice, DDWs have not been used for this purpose. AFP has indicated that 'taking down' of offensive material (such as child abuse material or objectionable violent material) is generally done in partnership with the eSafety Commissioner and/or industry partners.[133]

127 Established as a virtual centre within the Australian Competition and Consumer Commission in 2023.
128 Relevant responsibilities include actions to limit or prevent crimes such as identity and financial theft perpetrated via telecommunications networks and services: *Telecommunications Act 1997* (Cth) s 312.
129 Responsible for taking of action under the *Online Safety Act 2021* (Cth).
130 Australian Human Rights Commission (AHRC), *Submission 21*, 14 [48].
131 Law Council, *Submission 23*, 25–26 [78]–[79]. The Law Council noted the introduction in March 2022 of Project REDSPICE, which was directed to a significant enhancement to ASD's cyber and intelligence capability.
132 Revised Explanatory Memorandum, 27 [46].
133 INSLM, *Summary of private hearing – AFP*, 23 July 2024, 2–3. However, there are a range of other circumstances where DDWs could be used where the eSafety Commissioner's takedown powers would not be available, including where DDWs have been used in practice.

5.8 ASD has undertaken disruptive activity in collaboration with AFP against international cybercriminal syndicates causing harm against Australians.[134] However, ASD's legislative remit means that it must stop any activity it is undertaking under its own legislation if it makes 'a reasonable assessment that that activity might involve an Australian person or be being conducted from a computer or network inside Australia.'[135] This limit is entirely appropriate given that ASD's primary role is that of a foreign intelligence agency, not a law enforcement agency. Data disruption inside Australia needs to rely on a DDW.

5.9 Other available mechanisms are not generally tailored to facilitating collection of evidence for criminal proceedings (as is the case with ATWs) or intelligence for law enforcement purposes (as is the case with NAWs). The effectiveness of regulatory mechanisms is also highly dependent on the behaviour of individual businesses and whether they are bound by the relevant Australian laws. These regulatory mechanisms may be less effective in combating large-scale and high-volume forms of cybercrime, such as the use of malware perpetrated by foreign actors.

5.10 Having reviewed the way that *SLAID Act* powers have been used in practice (Chapter 4), it is clear they have been used in circumstances where other warrants would have been ineffective and where regulatory action would have been insufficient.

5.11 Therefore, I am satisfied that there is an ongoing need for some form of the *SLAID Act* powers as part of the government's response to what ASD has described as the 'ever changing cyber threat landscape.'[136] Given their unique characteristics, all 3 powers are likely to continue to be used in situations where other mechanisms would be ineffective in combating cybercrime. However, if the warrants are to be retained the system of safeguards needs to be updated. Later chapters propose important changes that are needed, particularly in the way that warrants are issued, to ensure that there are appropriate safeguards if *SLAID Act* powers are to continued.

There is an ongoing need for *SLAID Act* powers in conjunction with other mechanisms for combating cybercrime. As discussed later in the report, some additional safeguards are required.

134 ASD, Submission No 26 to PJCLE, Parliament of Australia, *Inquiry into capability of law enforcement to respond to cybercrime* (December 2023) 2; AFP, 'AFP Takes the Fight to Cybercriminals in 2024' (Media Release, 30 December 2024).

135 Evidence to PJCIS, Parliament of Australia, Canberra, 10 March 2021, 63 (Rachel Noble, Director-General, ASD). This does not preclude ASD providing assistance to AFP for operations on computers or networks inside Australia on the basis of an AFP warrant.

136 ASD, *Annual Cyber Threat Report 2023–24* (Report, 20 November 2024) 33.

Which agencies should be able to exercise SLAID Act powers?

5.12 Although I am satisfied that there is an ongoing need for *SLAID Act* powers more generally, a separate question arises as to which agency should be able to exercise which powers. This section of the report considers whether both ACIC and AFP should retain each individual *SLAID Act* power.

5.13 No submissions were made that proposed extending *SLAID Act* powers to state or territory police. Any proposal to do so would require careful consideration. Similarly, there were no submissions that proposed extending the powers to ASIO. Again, this type of proposal would require careful consideration, particularly for DDWs and ATWs.

Data disruption powers

5.14 As outlined in Chapter 4, ACIC has not sought any DDWs. In its original submission to this review, while noting that making *SLAID Act* powers operational 'had taken significantly longer than originally anticipated,' ACIC said it was anticipated that 'investment will support development of the data disruption capability,' and continued access to DDWs was 'necessary and appropriate for the agency's current and future approach to addressing TSOC [transnational, serious and organised crime].'[137]

5.15 Specifically, ACIC submitted that:

> DDWs would enable the ACIC to exploit existing relationships within and between TSOC groups and entities by authorising the agency to interfere with the data held on online criminal networks or devices for the purposes of frustrating the commissioning of serious criminal offences.[138]

5.16 Since that ACIC submission was made, the government has released the report of the ACIC Review. One of the conclusions of that review was that 'disruption activities go beyond the ACIC's intelligence functions and should be the preserve of law enforcement and other appropriately authorised agencies.'[139] The government supported the ACIC Review's recommendation that ACIC not have the legal function of undertaking operations that are primarily designed to disrupt criminal activities.[140]

A recent review of ACIC concluded it should not undertake disruption activities.

137 ACIC, *Submission 17*, 3.
138 ACIC *Submission 17*, 3.
139 *ACIC Review* 32.
140 *Government response to the ACIC Review* 8.

5.17 Many non-government submissions to this review said that there was not a compelling case for ACIC to maintain DDWs.[141] For example, Dr Brendan Walker-Munro said:

> As the ACIC is not a law enforcement agency in the same category as the AFP, the ACIC should not be gathering evidence relating to the commission of offences. The ACIC thus should not have access to DDWs or ATWs, unless these activities are led by the AFP under the imprimatur of an investigation into alleged offending.[142]

5.18 When explaining why it should retain DDWs, noting the government's acceptance of the ACIC Review recommendation, ACIC sought to distinguish between the disruptive effect of intelligence operations and the traditional definition of disruption as it applies to law enforcement.[143] ACIC also suggested timeliness and system compatibility issues as additional reasons ACIC should continue to have direct access to DDWs rather than cooperating with AFP if a disruption was necessary.

Recommendation on data disruption powers

5.19 As outlined above, I am satisfied that there is an ongoing need for DDWs. In finding that they are still needed, I am conscious that DDWs are a highly unusual power and one that should be used as little as possible. Using an otherwise unlawful activity (or taking otherwise unlawful action) to disrupt crime is an extension of the law enforcement function of police. That type of action should be used only after police have considered other more traditional law enforcement responses, including prosecution. Wherever possible, ordinary criminal law enforcement methods should be used. Prosecution allows an accused person procedural fairness in a way that a DDW cannot (see Chapter 11, where I recommend DDWs only be available as a 'last resort.')

5.20 Undertaking disruption that is otherwise unlawful is not an intelligence collection or analysis activity. Separating otherwise unlawful disruption activity from police risks overuse, or use in isolation from ordinary law enforcement methodology. I recognise that intelligence operations may have a disruptive effect; however, there is a clear distinction in law between disruption of criminal activity as an end to itself and the incidental disruption of this activity resulting from proper intelligence collection activities.[144]

5.21 Therefore, I am strongly of the view that use of DDWs should be limited to AFP.

---

141 QCCL, *Submission 6*, 5–6; Philip Glover, *Submission 8*, 3; New South Wales Council for Civil Liberties (NSWCCL), *Submission 10*, 3; Law Council, *Submission 23*, 31–2 [98]–[103] Recommendation 8.

142 Brendan Walker-Munro, *Submission 3*, 3. See also QCCL, *Submission 6*, 5–6; Philip Glover, *Submission 8*, 3; NSWCCL, *Submission 10*, 2; Digital Rights Watch, *Submission 22*, 5.

143 Heather Cook, CEO, ACIC, *Public hearing transcript*, 20 February 2025, 49–51. See also *ACIC Review* 23–4, 31–2.

144 For example, ASIO engages in incidental disruption of foreign interference activities by conducting overt intelligence-led activities such as conducting voluntary interviews, conducting overt entry-and-search operations (under warrant) and by executing compulsory questioning warrants: Evidence to Senate Legal and Constitutional Affairs Committee, Parliament of Australia, Canberra, 27 March 2025, 111 (Mike Burgess, Director-General of Security).

5.22 I also note that if ACIC were to retain the ability to exercise data disruption powers, it would be inconsistent with the ACIC Review recommendation, supported by government, that ACIC should not have functions primarily designed to disrupt criminal activities.

5.23 AFP provided evidence to this review that indicates there are considerable costs and resourcing requirements associated with developing and implementing the DDW capability. ACIC has not yet operationalised DDWs, and the investment of considerable time, money and resources would be required for them to do so.

5.24 It was unclear from the hypothetical cases that ACIC provided why it would not be possible for it to work collaboratively with AFP and rely on AFP's capability in these cases. Incompatibility of systems and competing agency priorities are not sufficient reasons for an agency to retain an extraordinary legal power like DDWs.[145] There are administrative mechanisms that enable agencies to work together to utilise the appropriate legal power and technical capability in joint operations.

5.25 I note ACIC's submission that it would be 'premature' to propose changes to ACIC's powers before the ACIC Review and electronic surveillance reform are implemented; and the AGD submission that ACIC should continue to have the 'appropriate powers to fulfil its existing functions.'[146] I find this unconvincing given government has accepted the recommendation that ACIC not have a disruption function; and because ACIC has been performing its existing functions without ever using a DDW.

5.26 Legislative amendments to remove ACIC's ability to use DDWs should be made as a priority, and certainly no later than the time the broader ACIC reforms are implemented. As described later in this report, the main safeguard for DDWs – the warrant issuing system – is currently not fit for purpose. If the recommended changes to the warrant issuing system (recommendations 6-8) are not implemented, DDWs should be allowed to sunset for both AFP and ACIC.

Recommendation 1: AFP should retain DDWs, subject to recommendations 6–8 being implemented. ACIC should not retain the ability to use DDWs.

145 See Wendy Darling, National Manager, ACIC, *Public hearing transcript*, 20 February 2025, 50–1.
146 ACIC, *Submission 17*, 6; AGD, *Submission 20*, 4–5.

Network activity powers

5.27 Both AFP and ACIC have used NAWs with good effect. As discussed in Chapter 4, NAWs have enabled ACIC to identify high-level criminal actors and previously unidentified criminal syndicates.[147] AFP has also used them for intelligence gathering on serious and organised crime, including crimes involving drugs, firearms, money laundering and people trafficking.[148] Based on evidence given in private hearings I am satisfied that these outcomes could not have been achieved using conventional warrants.

Recommendation on network activity powers

5.28 Given ACIC's specialist role as a criminal intelligence agency and the ACIC Review, which makes clear that this is to be the key role of the agency, there is little doubt that ACIC should retain NAWs, subject to improved safeguards.

5.29 Although the ACIC Review recognised the importance of reducing duplication of criminal intelligence efforts, it acknowledged that it would still be necessary for AFP to continue to undertake operational and tactical intelligence functions; this is despite ACIC having primary responsibility for intelligence functions.[149] In light of this conclusion, and evidence that AFP use NAWs effectively and differently from ACIC, I am satisfied there is an ongoing need for AFP to use network activity powers to support their law enforcement functions.

5.30 As described later in this report, the main safeguard for NAWs – the warrant issuing system – is currently not fit for purpose. If the recommended changes to the warrant issuing system (recommendations 6-8) are not implemented, NAWs should be allowed to sunset for both AFP and ACIC.

Recommendation 2: ACIC and AFP should retain NAWs, subject to recommendations 6–8 being implemented.

147 Heather Cook, CEO, ACIC, *Public hearing transcript*, 20 February 2025, 42.
148 INSLM, *Summary of private hearing – AFP*, 23 July 2024, 3.
149 *ACIC Review* 21.

Account takeover powers

5.31 AFP has used account takeover powers to good effect. The warrants have provided clear authority to 'take over' accounts that AFP reasonably believed were being used for criminal purposes. The 'takeover' has allowed other powers – for example, search warrants – to be used to gather admissible evidence from those accounts. The ability to take over accounts 'locks out' the account holder and prevents evidence from being deleted or modified while a search warrant or other power to copy data is exercised. In some cases, controlled operation authorities may also be used to operate an account to gather further evidence. A strong case was made, including in public and closed hearings, about how AFP has used these warrants. I am satisfied that AFP requires ongoing access to ATWs, subject to improvements to safeguards.

AFP should have ongoing access to account takeover powers.

5.32 ACIC has not sought any ATWs. Many stakeholders argued that ACIC did not have an ongoing need for ATWs. For example, the Law Council of Australia said:

> The eligibility to apply for [ATWs] should be confined to the AFP because of the ACIC's role as a criminal intelligence agency that collaborates with the AFP to support AFP-led cybercrime related disruption operations.[150]

5.33 In response to questions about the ongoing necessity of ATWs for its agency, ACIC submitted that these warrants:

- remain 'relevant and appropriate' for the agency despite them not being used to date
- would complement traditional methods to infiltrate TSOC groups to understand the threat they pose to Australia – for example, by enabling the agency to exploit existing relationships by authorising it to assume the personas of TSOC groups and entities through their internet accounts
- were likely to be used infrequently '[but] this does not mean however that the power is inappropriate or disproportionate.'[151]

150 Law Council, *Submission 23*, 31 [98].
151 ACIC, *Submission 17*, 5.

5.34 Information provided to this review also indicated that ACIC proposed to use ATWs in a covert manner.[152] This contrasts with AFP's use of ATWs in conjunction with overt search warrants.[153]

5.35 In a private hearing ACIC subsequently provided several examples of their proposed use of ATWs. These included situations where they considered that they would be able to take over and operate an account for a short period of time using an ATW covertly in conjunction with their other powers.[154] Some of the details ACIC provided cannot be included here, as to do so would risk compromising current and planned operations However, the scenarios described feasible situations where ACIC could take over an online account for a short period, including:

- where it takes over and then covertly operates an account, using a combination of its existing powers plus an ATW, to gather information
- where other intelligence indicates the owner of the account was unlikely to discover that their account had been taken over
- to make later evidence collection under other powers more effective.

5.36 ACIC also gave a hypothetical example of working with a service provider, such as a financial services provider, where it believed that the use of an ATW would allow it to obtain evidence that could not be gathered using a search warrant.[155]

Recommendation on account takeover powers

5.37 Although I was initially of the view that ACIC should not retain the ability to use ATWs, after considering additional information that was provided in a private hearing with ACIC, I am satisfied that there is a case for ACIC to retain an account takeover power similar to an ATW. However, the purpose of this type of power in the context of ACIC (as compared to AFP) should be more aligned with their role as a criminal intelligence agency.

5.38 As recognised by the ACIC Review, the legislative framework that applies to ACIC does not clearly align with their role as a criminal intelligence agency.[156] Most of ACIC's current covert collection powers (including ATWs) are based on the premise that it is a law enforcement agency whose functions include enforcing the criminal law and obtaining evidence.[157] To address this discrepancy between ACIC's legislative framework and its actual future role, the ACIC Review recommended that ACIC's ability to use covert collection powers be aligned with the agency's

152 INSLM, *Summary of private hearing – ACIC*, 11 March 2025, 2.
153 Prior to the implementation of the *SLAID Act*, AFP provided the PJCIS hypothetical case studies that included use of an ATW in both an overt and a covert manner. AFP, Submission No 6 to PJCIS, Parliament of Australia, *Review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (February 2021) 13–17.
154 See INSLM, *Summary of private hearing – ACIC*, 11 March 2025, 2–3.
155 INSLM, *Summary of private hearing – ACIC*, 11 March 2025, 3.
156 *ACIC Review* 18–19.
157 *ACIC Review* 23. NAWs are an exception to this.

intelligence function.[158] The government accepted this recommendation.[159]

5.39 Consistent with this recommendation, amendments should be made so that ACIC is able to take over an online account to enable it to collect criminal intelligence. The existing requirement to obtain another authority to conduct other activities, including the operation of the account to collect intelligence, should continue to apply.

5.40 As described later in this report the main safeguard for ATWs – the warrant issuing system – is currently not fit for purpose. Subject to the recommended changes being made to that system (recommendations 6-8), I am satisfied that there is a case for account takeover powers to continue to be available to both AFP and ACIC.

5.41 Changes to align ACIC's use of ATWs with their intelligence role could logically be made at the same time as other amendments to implement the ACIC Review. Regardless, if the other changes to the system for issuing warrants recommended in this report are not implemented, the ATW provisions for AFP and ACIC should be allowed to sunset.

Recommendation 3: Both ACIC and AFP should retain ATWs, subject to recommendations 6–8 being implemented.

In the case of ACIC, ATWs should be for intelligence rather than evidence collection purposes.

158 *ACIC Review* 25 Recommendation 4.
159 *Government Response to the ACIC Review* 6.

Chapter 6: Operational improvements

6.1 During this review, agencies suggested several changes that could be made to improve what they described as the 'operational effectiveness' of *SLAID Act* warrants. In this chapter I specifically address these proposals.

6.2 The 2 specific changes that I support are:

- introducing named person ATWs
- extending the maximum duration of NAWs to 6 months.

6.3 My support for these changes is contingent on the adoption of other changes recommended in this report to enhance the safeguards that ensure extraordinary powers are exercised in a proportionate way. I note that some of these other changes will also improve the operation and effectiveness of *SLAID Act* powers – for example, by providing for a system for consistent, timely processing of applications (as discussed in Part 3) and streamlining issuing criteria (Chapter 11).

6.4 Agencies proposed 2 additional potential 'enhancements': extending the scope of NAWs to include additional electronic surveillance capabilities; and removing extraterritorial limits on NAWs and DDWs. The first of these proposed changes is discussed below and the latter in Chapter 18. I do not recommend either of these proposals be adopted.

Named person ATW

6.5 A single ATW can currently authorise taking over multiple accounts but only if each account is known and specified in the warrant at the time it is issued. AFP said in its submission that this has created difficulties in practice, because 'if additional accounts are identified, once a device has been accessed, investigators must apply for a further ATWs [sic].'[160] During the public hearing AFP described a situation where this had arisen. While executing an overt search warrant and an ATW at premises associated with a person suspected of committing a serious crime, investigators identified further accounts used by the same individual and suspected they were being used for the same alleged offending.[161]

6.6 If a person is not promptly 'locked out' of an account identified during an overt search they may be able to access it and delete evidence, or have someone else do that for them. Some online accounts can be deleted remotely.[162] I was also advised that some types of online accounts that are often involved in particular types of offending will 'self-delete' if they have not been used for quite short periods of time. In this context I accept that there may be situations where there is a real risk evidence will be lost before police can obtain an urgent warrant for the newly identified account (or an emergency authorisation if the criteria are satisfied – see Chapter 13.

160 AFP, *Submission 18*, 7 [39].
161 Rob Nelson, Commander, AFP, *Public hearing transcript*, 20 February 2025, 34–5.
162 AGD, *Submission 20*, 7.

6.7 Both AFP and AGD suggested that these difficulties could be addressed by enabling agencies to seek a warrant authorising the takeover of any accounts being used by a person specified in the warrant ('a named person ATW').[163] This would allow for accounts to be 'added' to the ATW after it has been issued, provided that they had the requisite link to the specified person. A similar mechanism currently exists for 'named person warrants' under the *TIA Act*.[164] In practice, AFP said that this would allow it to take actions such as changing the password to an account to prevent others from accessing it and deleting the content before evidence can be collected.[165]

6.8 Non-government submissions expressed some concerns about the proposal for a named person ATW, highlighting the need for additional safeguards to ensure that the exercise of the power remained necessary and proportionate.[166] The Law Council of Australia noted that a named person ATW would in practice authorise a very broad range of actions given the breadth of the definition of an 'online account.' It emphasised the need for a clear link between the account being taken over and the suspected offending conduct.[167]

> The case AFP made for named person ATWs was convincing, but additional safeguards are needed if the warrants are to be expanded in this way.

6.9 I found the case AFP made for named person ATWs to be convincing. The unique nature of online accounts, including the way that they can be deleted remotely or set to self-delete means that there is a real risk of losing evidence, despite an issuing authority already being satisfied the individual should be the subject of an ATW. I also found the concerns raised by the Human Rights Commissioner and the Law Council to be well made. It is true that named person ATWs would effectively give agencies the ability to vary the scope of the warrant without having to go back to the issuing authority. This makes the warrants more invasive than they currently are and emphasises the need for effective safeguards.

163 AFP, *Submission 18*, 7 [40]; AGD, *Submission 20*, 6–7.

164 See ss 9A, 11B and 46A of the *TIA Act*, which provides for a warrant authorising the interception of any telecommunications service a person is using or is likely to use. Warrant applications must list (to the extent known) the services that the person is using, or is likely to use: ss 9A(2), 11B(2), 42(4A). Where it is proposed to intercept a telecommunications service that was not specified in the warrant, a senior 'certifying person' or 'certifying officer' of the relevant agency must cause an authorised representative of the carrier to be given a description of the service: ss 16, 60(4)–(4A). Records of all intercepted services must be kept and including in reports to the Minister: ss 81(1)(c), 81(2), 81A(2)(e), 94B.

165 Rob Nelson, Commander, AFP, *Public hearing transcript*, 20 February 2025, 35.

166 Lorraine Finlay, Human Rights Commissioner, *Public hearing transcript*, 19 February 2025, 13; Keiran Hardy, *Public hearing transcript*, 19 February 2025, 61.

167 Lloyd Babb, *Public hearing transcript*, 19 February 2025, 53–4.

6.10 Noting that it has not sought any ATWs, ACIC did not suggest a similar change or give evidence that it anticipated facing challenges similar to those faced by AFP. This may be explained by the different proposed use for ATWs by ACIC as compared to AFP. For example, unlike AFP's use of an overt ATW in connection with a search warrant, ACIC gave evidence its proposed use of ATWs would be to 'more covertly intercept or penetrate' an account.[168] The proposed change to ACIC ATWs to focus them on 'intelligence' rather than evidence means that, in the early stages of an intelligence operation, ACIC may have identified a specific person but not know all of the accounts that they use to engage in suspected unlawful activity. The safeguards identified below, together with the proposed new system for issuing warrants (see Part 3) are intended to ensure that named person ATWs are not the 'default' option but are only used where standard ATWs would be impractical or ineffective. ACIC should also have access to named person ATWs where the additional safeguards are satisfied.

Account takeover warrants for specified accounts would be ineffective

6.11 Given their broader scope, named person ATWs should not be available by default, and agencies should demonstrate to the issuing authority why obtaining a specified account ATW would be ineffective in the circumstances.[169] Similar requirements currently exist for named person warrants under the *TIA Act*[170] and were recommended for group electronic surveillance warrants in the 2019 Comprehensive Review.[171]

6.12 The exact wording is a matter for drafters, but my intent is that agencies would have to demonstrate that an account-based warrant, or multiple account-based warrants, would be impractical or ineffective. This is intended to be a significantly higher standard 'inconvenience.' If it is likely that all relevant accounts can be identified or there is not a real risk that evidence (or, for ACIC, intelligence) may be deleted before an urgent warrant variation can be sought then a named person warrant should not be available.

Accounts used by an individual – not every account an administrator could access

6.13 Although there is a requirement for an ATW to specify the holder or users of target accounts to the extent this is known to the applicant agency, the accounts that may

168 Heather Cook, CEO, ACIC, *Public hearing transcript*, 20 February 2025, 52.
169 See also *2019 Comprehensive Review*, vol 2 341 [28.244].
170 *TIA Act* s 46A(1)(c). Note differences in tests for ASIO (Attorney-General needs to be satisfied service warrant would be ineffective) and law enforcement (issuing authority needs to be satisfied likely to use multiple services and have regard to availability of other mechanisms including service warrant).
171 *2019 Comprehensive Review*, vol 2, 293, Recommendation 83.

be specified in an ATW are not currently limited to accounts that are all used or held by a particular person.[172]

6.14 Similar to named person warrants under the *TIA Act*, a named person ATW should only authorise the taking-over of an account where there are reasonable grounds for suspecting that the named *individual* is using, or is likely to use, that account. Conditions should be considered where there is evidence that other people may use the account.

6.15 Agencies should not be able to use a named person ATWs in a way that allows them to take control of accounts used by many different people. For example, they should not enable an agency to name a network administrator and then take over accounts used by other unknown individuals that a system administrator could access because they are an administrator.

Certification process for adding accounts not specified in the warrant

6.16 I acknowledge that there is scope for a named person ATW to authorise a broad range of actions, given the breadth of the definition of 'online account.'

6.17 There are existing requirements in the *Crimes Act* that operate to limit the accounts that can be taken over under an ATW. This includes the requirement for the issuing authority to be satisfied that there are reasonable grounds for the suspicion that taking control of the target account(s) is necessary for the purpose of enabling evidence to be obtained of the commission of relevant offences. In addition, the authority to take control of an account is limited to circumstances where doing so is *necessary* to obtain evidence of the commission of the alleged relevant offending in respect of which the warrant is issued.[173]

6.18 Mechanisms should be put in place to ensure that accounts are only added to a named person ATW where:

- there is a link between the account and the obtaining evidence of (or, for ACIC, intelligence about) the commission of the relevant offences in respect of which the warrant is issued; and
- it is necessary and proportionate to do so.

6.19 This could be achieved by introducing a requirement to follow a certification process before taking over accounts that are not specified in the warrant. To provide greater transparency and accountability, this requirement should be set out in the legislation rather than solely through administrative arrangements.

172 *Crimes Act* ss 3ZZUQ(1)(b)(vii)–(viii).

173 *Crimes Act* ss 3ZZUP(1), 3ZZUR(2)(a). For ACIC, this would become necessary for obtaining intelligence about commission of a relevant offence if Recommendation 3 is accepted.

6.20 This type of requirement should provide that an account not specified in the ATW can only be taken over where a senior officer is satisfied of *all* following:[174]

- They suspect, on reasonable grounds, that the *individual* specified in the warrant is using or likely to be using the account (see above re network administrators).
- They suspect, on reasonable grounds, that it is necessary to take control of the account to enable collection of evidence of (or, for ACIC, intelligence about) the commission of the relevant offending that the warrant is to identify.
- They are satisfied that taking control of the account is proportionate, having regard to the factors that an issuing authority would have to have regard to when issuing an ATW under the Act.[175]

6.21 There should also be a requirement for the certifying officer to make a written record and reasons for their decision. That record will be an important part of the scrutiny that the relevant oversight body will apply if they inspect the warrant.

Additional reporting requirements

6.22 Similar to existing requirements for named person warrants under the *TIA Act*, there should be a requirement for the report given to the Minister to include information about the accounts that were taken over under the warrant and the reasons it would not have been effective to take over those accounts under a specified account ATW.[176]

6.23 There should also be public reporting about the number of accounts taken over under named person ATWs.[177] See Chapter 15 on proposed improvements to reporting requirements.

Recommendation 4: Named person ATWs should be introduced for AFP and ACIC subject to recommendations 6–8 and the following additional safeguards:

(a) Available only where the use of an account-based ATW would be ineffective.

(b) A certification process for adding accounts based on the same criteria used to issue ATWs.

(c) Additional record keeping and reporting requirements.

174 The certifying officer should be at least a senior executive level office nominated by the agency head. This is consistent with certifying officers under the *TIA Act* s 5AC.

175 See the proposed improvements to issuing criteria in Chapter 11.

176 *TIA Act* s 94B.

177 Similar to named person warrants reporting requirements under s 100 of the *TIA Act*.

Extending maximum duration of NAWs

6.24 Like most law enforcement related warrants, NAWs can be issued for a maximum of 90 days.[178] NAWs can be extended for a further 90 days, with no limitations on the number of extensions.[179] In practice, NAWs have been frequently and repeatedly extended, reflecting their use as a criminal intelligence tool and the fact that intelligence operations often run for extended periods of time. Other intelligence warrants, including ASIO surveillance device warrants, are available for a period of up to 6 months.[180] Unlike NAWs, ASIO warrants cannot be extended beyond the maximum 6-month duration, but a new warrant may be issued for the same target or circumstances.[181]

6.25 ACIC submitted that extending the duration of NAWs to align with other intelligence authorities 'would enhance operational planning and effectiveness of the authority.'[182] ACIC also noted that 'significant time is required once a warrant is issued to identify, assess, develop and test the technical options available prior to operational activity occurring' and '[t]he collection of intelligence on complex criminal intelligence networks also frequently demands protracted periods of collection activity.'[183]

> Intelligence collection, particularly of the type undertaken by ACIC using NAWs, can take an extended period of time.

6.26 AGD supported this proposal. It noted that a longer period would reflect 'the typically longer duration of intelligence-collection operations, which often have broader and long-term objectives compared to evidential investigations.'[184] AFP, while not expressly supporting an extension of the maximum duration, noted that the increased complexity and size of criminal networks requires sufficient time to execute warrants and enable an informed assessment.[185] AFP initially commented that there was some benefit in ensuring alignment with parallel law enforcement warrant timeframes.[186] However, it later said that extending the duration of NAWs to 6 months was 'worthy of further discussion.'[187]

178 *SD Act* s 27KN(2).
179 *SD Act* s 27KQ(1), (6).
180 ASIO warrants can be varied to extend the period during which the warrant is in force, but this must not exceed the relevant maximum duration for that warrant: *ASIO Act* s 29A(3).
181 See, for example, *ASIO Act* s 26A(4).
182 ACIC, *Submission 17*, 8. ACIC suggested extending NAWs to 6 to 12 months.
183 ACIC, *Submission 17,* 8.
184 AGD, *Submission 20*, 5.
185 AFP, *Submission 18*, 6 [34].
186 INSLM, *Summary of private hearing – AFP*, 23 July 2024, 3.
187 Ian McCartney, Deputy Commissioner, AFP, *Public hearing transcript*, 20 February 2025, 35.

Risks associated with a longer network activity warrant

6.27 Non-government submissions and the Human Rights Commissioner said that an increase to the maximum length of a NAW should be approached with caution.[188] For example, while acknowledging the practical concerns that ACIC and AGD raised, the Human Rights Commissioner considered there would need to be 'robust safeguards' in place for any extension of time, given the 'extraordinary nature of these powers and recognising the fact that they are already extremely powerful tools.'[189] Lloyd Babb SC on behalf of the Law Council of Australia 'strongly opposed' the suggested change given the requirement to return to the issuing authority is an important safeguard and because of concern about the breadth and 'anticipatory nature' of NAWs.[190]

Revocation of warrants that are no longer required

6.28 Increasing the maximum duration of a warrant increases the risk that a warrant may be left in place when it is not actually required. It is a current requirement that collection cease and warrants be revoked by the chief officer of ACIC or AFP where satisfied that access to data under the warrant is no longer required.[191] The Commonwealth Ombudsman (the Ombudsman) has made recent adverse findings about both AFP and ACIC's compliance with similar requirements for other *SD Act* warrants. For example:

- AFP took longer than 28 days to revoke surveillance device warrants in 5 instances where the warrant was 'no longer required for the purpose for which it was sought.'[192]
- ACIC failed to execute warrants during the 90-day period in 3 of the 5 warrants inspected. There were no records of any review or decision to retain the unexecuted warrants.[193]

188 Lorraine Finlay, Human Rights Commissioner, *Public hearing transcript*, 19 February 2025, 14; Rebecca Ananian-Welsh, *Public hearing transcript*, 19 February 2025, 62; Lloyd Babb, *Public hearing transcript*, 19 February 2025, 55.

189 Lorraine Finlay, Human Rights Commissioner, *Public hearing transcript*, 19 February 2025.

190 Lloyd Babb, *Public hearing transcript*, 19 February 2025, 55.

191 *SD Act* ss 27KR(2), 27KS.

192 Commonwealth Ombudsman, *Report to the Attorney-General on Agencies' Compliance with the Surveillance Devices Act 2004 (Cth) for Ombudsman Inspections Conducted from 1 July to 31 December 2023* (Report, 1 March 2024) 15. It is noted that the 28-day period is not a statutory requirement but a metric used by the Commonwealth Ombudsman (the Ombudsman) as part of their inspections.

193 Commonwealth Ombudsman, *Report to the Attorney-General on agencies' compliance with the Surveillance Devices Act 2004 (Cth) for Ombudsman inspections conducted from 1 July to 31 December 2023* (Report, 1 March 2024) 16.

6.29 In the context of the proposal to extend the duration of NAWs, I raised these Ombudsman findings in the public hearing. ACIC advised:

> Well, obviously, if that were the new policy or the legislative reform, we would put in we would need to put in place internal mechanisms. And we've certainly been responsive to the [Ombudsman's] findings and suggestions in regard to the surveillance device material …. But if the legislation were to change and this would be the new regime that would put in place, we would adjust and alter our internal policies and procedures to ensure that [at] a regular interval in between in [sic] that warrant period…we would be evaluating whether or not the warrant was still producing valuable…intelligence, still required and whether or not it needed to be revoked within that period.[194]

If the length of duration of NAWs is to be increased, it is particularly important to establish procedures to ensure that the need to continue a warrant is evaluated regularly.

6.30 Currently, an issuing authority has no real way of knowing whether warrants are being revoked by the chief officer as required. As discussed in Chapter 8 there is a need for relevant oversight findings to be communicated to issuing authorities.

Reporting is currently delayed by multiple renewals

6.31 Some NAWs appear to have been renewed at least 6 times, meaning no report has been provided to the Minister or been made available to oversight bodies in almost 2 years.[195]

6.32 The *SD Act* requires each agency to report to the relevant Minister on the details of a NAW as soon as practicable *once a warrant or authority has ceased to have effect*.[196] As noted by the Inspector-General of Intelligence and Security (IGIS), the lack of any upper limit on how many times a 90-day NAW can be renewed may result in 'an extended period of time in which the Minister is not being provided any substantive information about the execution of the warrant.'[197] In addition, as these reports form an important component of the inspections undertaken by oversight agencies, delays in reporting to the Minister have practical flow-on effects for the timing and frequency of oversight inspections.

194 Heather Cook, CEO, ACIC, *Public hearing transcript*, 20 February 2025, 53.

195 Based on public reporting, in the 3 years to 30 June 2024 AFP was issued with 4 NAWs and received 10 extensions, while ACIC was issued with 3 NAWs and received 6 extensions: *SD Act Annual Report 2022–23*, 31; *SD Act Annual Report 2023–24*, 30. In the 6 months from 1 July 2024 to 31 December 2024, neither agency was issued a new NAW however AFP received 3 extensions and ACIC received 2 extensions (see Tables 1 and 2 in Chapter 4). Based on the statistics in those tables, it appears there is one ACIC NAW that has been renewed at least 6 times.

196 *SD Act* s 49.

197 IGIS, *Submission 9*, 5 [20].

The absence of a limit on the number of times a NAW can be renewed is problematic because the requirement to report is not triggered until the warrant ceases to have effect.

6.33 In response to a request for the Inspector-General's views about the proposal to extend the maximum duration of NAWs, the IGIS noted that requiring a report to be provided every 6 months would address the concerns in his original submission to this review regarding the current timing of ministerial reporting on individual warrants.[198] The Ombudsman separately advised that he has 'no concerns' with the proposed extension to 6 months, 'subject to those warrants not being renewable and also the additional proposed safeguards.'[199] A requirement that warrants not be renewable does not mean warrants should not be able to be reissued under a fresh application in respect of the same targets. Instead, the point here is that a fixed maximum warrant duration creates a definite point in time at which a detailed report on the warrant is prepared.

6.34 AGD observed that a requirement to apply for a new warrant after 6 months may have its own adverse consequences for the reporting framework:

> Removing extensions and requiring agencies to obtain a new warrant would limit public visibility of the extent to which warrants are renewed or extended, and potentially lead to an inaccurate perception that a larger number of distinct warrants are being issued.[200]

6.35 I consider that concerns about inaccurate perceptions of the number of warrants being issued can be addressed by ensuring that public reporting describes how warrants are being used, including where multiple warrants are sought for the same or similar subject matter as part of a longer-term operation.[201]

6.36 ACIC said that, if NAWs were extended but not renewable (like ASIO warrants), this would meet ACIC's needs, although it suggested a 6–12 month timeframe:

> [We] would certainly be open to considering that sort of a reform and what you proposed around that six to twelve months and having to close off and issue a new warrant wouldn't pose a difficulty for us.[202]

198 IGIS and INSLM, *Agreed Record of Meeting* (28 February 2025).
199 Letter from Ombudsman to INSLM, 31 March 2025.
200 AGD, *Supplementary submission 28*, 6.
201 AGD, *Supplementary submission 28*, 6.
202 Heather Cook, CEO, ACIC, *Public hearing transcript*, 20 February 2025, 53.

Recommendation on extending the maximum duration of NAWs

6.37 Any decision to extend the maximum duration of warrants authorising the use of covert and intrusive powers should not be taken lightly. This is particularly the case with NAWs, given their potential to be used to collect significant amounts of information, including about individuals who are not directly involved in the suspected criminal activity.

6.38 I am satisfied that there is a case for the extension of the maximum duration of NAWs given the longer term nature of intelligence operations. I therefore support the proposal to extend the maximum duration of NAWs to 6 months. However, it is important that a full report on each NAW be provided to the relevant Minister (and also the relevant oversight body) at least every 6 months. It is also essential that effective safeguards are in place, especially a new system for issuing warrants that is fit for purpose (see Part 3).

6.39 My preferred mechanism for 6-month NAWs would be to make NAWs non-renewable, like ASIO warrants. However, I recognise that in the alternative the same effect could be achieved by requiring that when a NAW is 'renewed' a report must be provided to the Minister (and relevant oversight body) – it should be the same detailed report that is currently required when a NAW ceases to have effect and any 'renewal' should be subject to exactly the same issuing criteria and issuing process as a new warrant.[203]

6.40 Increasing the *maximum* duration to 6 months does not prevent an agency from seeking a warrant for a shorter time – for example, if a longer warrant is unnecessary or it is determined that a NAW should align with the shorter cycle of other law enforcement powers that may be in use for an operation (as noted above in relation to AFP). If an agency is issued a warrant for less than 6 months and then extends the warrant, it should still be required to provide a full report at the 6-month mark.

6.41 If issuing authorities are to be asked to issue NAWs for 6 months, the safeguards recommended in this report and particularly recommendations 6-8 need to be implemented. If they are not then NAW powers should be allowed to sunset.

Recommendation 5: The maximum duration of NAWs should be extended to 6 months, subject to recommendations 6–8 being implemented and a mechanism to ensure 6-monthly reporting.

6.42 Reporting requirements are discussed further in Chapter 15 and recommendation 19.

203 See Chapter 15 for further discussion about the frequency and content of reporting.

Extending scope of NAWs

6.43 NAWs authorise the use of computer access capabilities to obtain data from the target computer/s. The use of surveillance devices or telecommunications interception may also be authorised, but their use must be limited to only what is necessary to achieve the computer access authorised by the warrant.[204] ACIC proposed extending the scope of NAWs to remove this limitation. This extension would allow a NAW to authorise the use of surveillance devices and telecommunications interception to gather intelligence on a large number of people, not all of whom are necessarily suspected of engaging in a crime. ACIC said this 'would enable the agency to use the least intrusive, most effective means possible to collect intelligence on a criminal network of individuals.'[205]

6.44 ACIC later clarified that it was primarily concerned about the consequences of the current inability to share information that had been collected under a NAW using telecommunications interception or surveillance device capabilities that were only used because it was necessary to do so to give effect to the warrant.[206] This separate issue is discussed in Chapter 12.

6.45 Extending the scope of the authority of NAWs so that a NAW could also allow the use of a surveillance device and telecommunications interception to intentionally gather intelligence would broaden ACIC's ability to collect intelligence on TSOC and, in that sense, improve the effectiveness of these warrants. However, it would significantly increase the scope and invasiveness of an already broad warrant and allow the use of surveillance devices and telecommunications interception to gather criminal intelligence at a lower threshold than has ever been permitted before.[207]

6.46 In this review, no compelling case was made that would justify departure from the existing express policy intent that:

- the authority under a NAW would be limited to access to data held on a computer
- separate warrants would be required to use telecommunications interception or surveillance device capabilities, other than to give effect to the NAW.[208]

6.47 Any consideration of an expansion of the authority under a NAW should be undertaken in the context of ESR and would require a robust system for issuing and reviewing warrants.

204 *SD Act* ss 27KP(2)(h), (i).
205 ACIC, *Submission 17*, 7.
206 INSLM, *Summary of private hearing – ACIC*, 20 February 2025, 3–4.
207 The Law Council also raised concerns about the approach taken for NAWs being replicated as part of the development of a group warrant framework: Law Council, *Submission 23*, 41–2.
208 Revised Explanatory Memorandum 98 [495], 102 [516]–[517].

Part 3. Warrant issuing system

The issuing of a warrant should not be regarded as a single action that occurs at a moment in time, carried out by an individual. It should be understood as a system that has many interconnected parts – for example, mechanisms to ensure access to complete and accurate information; issuing authorities with independence and appropriate skills, knowledge and training; opportunity for independent submissions and technical advice; and a structure that ensures there is time to consider applications in a timely way and where there is no room for a perception that applicants can or do select who considers their application.

This system is the most important safeguard for rights and promoting public confidence in the use of invasive powers by law enforcement and criminal intelligence agencies. As the joint academics said, '[t]he issuing stage is the most critical point for the appropriate balance to be struck between security and rights.'[209]

The current system for issuing electronic surveillance and *SLAID Act* warrants is decades old and is modelled on even older arrangements for issuing physical search warrants. This review provided an opportunity to test whether that system is as effective as it can be in the modern context of highly intrusive and often covert and technically complex powers that are unlikely to be challenged in a court. The review found it is not.

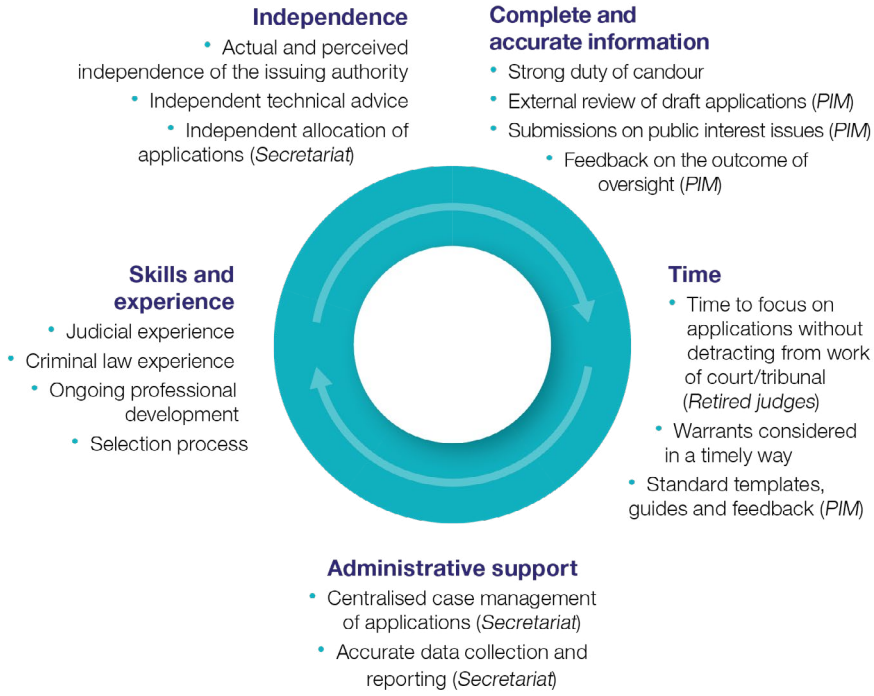
There are several areas in need of reform, such as access to independent technical advice; the inclusion of outcomes of oversight inspections in the information available to an issuing authority; the lack of a strong statutory duty of candour; and the introduction of a public interest monitor (PIMs) to provide feedback on draft applications and make submissions on public interest where appropriate. There are also gaps in consistency of applications, processes, data collection and access to continuing education. There are also currently insufficient mechanisms to guard against actual or perceived 'forum shopping.'

The current arrangement of relying primarily on Administrative Review Tribunal (ART) members to do the work of issuing warrants is also problematic including because ART members do this work in their personal capacity on top of the core work of the Tribunal: reviewing administrative decisions. The time taken to issue warrants detracts from ART's ability to manage its actual caseload and contributes to a growing backlog of cases.

This Part begins with the question of who should authorise warrants (Chapter 7). It then discusses how the introduction of PIMs is crucial to ensuring that issuing authorities are in the best position to make informed and balanced decisions (Chapter 8). It concludes with a discussion of other changes, such as access to independent technical advice, an enhanced duty of candour and better mechanisms for supporting issuing authorities and managing applications (Chapter 9).

209 Rebecca Ananian-Welsh, Tamara Tulich, Keiran Hardy, Peter Greste, Ausma Bernot and Danielle Ireland-Piper, *Submission 15* (Joint Academic Submission) 8.

Figure 1 – Proposed new system for issuing ESR and SLAID Act warrants



The review proposes a new system that would consist of a panel of retired judges as the issuing authorities, supported by PIMs. PIMs would have the ability to provide feedback and make submissions on matters of public interest as well as incorporate the findings of oversight agencies into those submissions. Independent technical advisors would be available for complex or novel matters and to increase knowledge of issuing authorities and PIMs. An independent secretariat would support the system, including by allocating warrants and collecting accurate data. Those applying for warrants would be subject to a statutory duty of candour.

In my view these changes are needed to make the warrant issuing system fit for purpose for technologically complex and invasive warrants such as those authorised under the *SLAID Act*. The proposed changes can also be expected to increase public confidence in the use of warranted powers for law enforcement and criminal intelligence. Implemented well, the changes should also make the process for seeking and properly considering warrants more efficient by providing feedback on draft applications, standardising templates, developing technical expertise and having dedicated issuing authorities readily available to consider applications in a timely way.

The financial cost of implementing the proposed system for issuing warrants should be modest and should be assessed in the context of the financial expenditure of police and criminal intelligence agencies exercising warrant powers as well as the benefit of increased rights protections and public confidence in the effectiveness of the critical safeguard that warrants provide.

Chapter 7: Who should issue warrants?

7.1 It is critical that the warrant system have the right set of people as issuing authorities. They need to have, and be seen to have, independence in decision-making. They also need to have, and be seen to have, appropriate skills and experience. Additionally, proper consideration of warrant applications takes time – and decisions need to be made in a timely way.

7.2 The person who makes the decision on whether a warrant should be issued is only one part of the overall system for issuing warrants. To be as effective and efficient as possible, issuing authorities need to be supported by mechanisms that include PIMs (Chapter 8), independent technical advice and a statutory framework that includes a duty of candour and independent allocation of warrants (Chapter 9), and appropriate issuing criteria (Chapter 11).

7.3 This chapter concludes that it is no longer appropriate to rely on members of ART to issue warrants. This is partly because of the burden that the issuing of warrants is placing on ART. It would be preferable if those issuing warrants were not doing so on top of an already busy workload. It is also desirable that they have experience in criminal law matters. To ensure public confidence in the system for issuing warrants, it is also necessary that those issuing warrants are perceived as having the gravitas to rigorously test police and criminal intelligence agency applications.

7.4 The highest level of confidence in the system for issuing warrants would result from being able to ask judges to issue all warrants and for them to be supported by PIMs and independent technical advice. However, it is impractical to have sitting judges issue all *SLAID Act* and electronic surveillance warrants. They may be able to issue *SLAID Act* warrants at the current volume, but this would still be an imposition on judicial time and is not the preferred solution. Magistrates issue physical search warrants, but *SLAID Act* warrants are in a different category. The potential technical complexity of *SLAID Act* warrants, including future uses of ATWs, means that they need particular experience and supports that it is not practical to provide all magistrates across the country. The preferred option is to instead rely on a panel of retired judges, potentially drawn from a broad range of state, territory and Commonwealth courts, to issue warrants.

Who issues SLAID Act warrants now?

7.5 Before looking at who should issue *SLAID Act* warrants, it is useful to first set out the evidence about who issues *SLAID Act* warrants now.

Who is authorised to issue SLAID Act warrants?

7.6 At present, the 'issuing authority' for DDWs and NAWs are 'eligible judges' and certain members of ART. The definition of 'eligible judge' includes members of the Federal Court of Australia (FCA) and Federal Circuit and Family Court of Australia

(FCFCOA) (Divisions 1 and 2).[210] ART members are eligible to become issuing authorities for DDWs and NAWs if they have been enrolled as legal practitioners for at least 5 years.[211] An eligible judge or ART member may be nominated as an issuing authority by the relevant Minister, although in the case of an eligible judge the Minister may only do so where the judge has consented in writing.[212] There is no equivalent consent requirement for ART members.[213] ATWs can only be issued by a magistrate.[214] Any magistrate can issue an ATW – they do not need to be nominated or appointed to do so.

7.7 Eligible judges who issue DDWs or NAWs, and magistrates who issue ATWs, are doing so in their personal rather than judicial capacity. This is due to constitutional constraints, discussed below. Non-judicial members of ART are also described as issuing warrants in their 'personal capacity,' although this is not for constitutional reasons.[215]

7.8 Currently, 55 judges and 41 ART members are authorised to issue DDWs and NAWs. Over 500 magistrates can issue ATWs. They are located around Australia.

There are 55 judges and 41 ART members who can issue DDWs and NAWs. Any magistrate can issue an ATW.

210 *SD Act* s 12. Federal Circuit and Family Court of Australia (FCFCOA) (Division 1) is a superior court; Division 2 is not: *Federal Circuit and Family Court of Australia Act 2021* (Cth) ss 9(1)(a), 10(1).

211 A full-time senior member who has been appointed on the basis of specialised non-legal expertise could theoretically be authorised to issue warrants: *SD Act* s 13. See also *Administrative Review Tribunal Act 2024* (Cth) ss 206–208 (*ART Act*).

212 *SD Act* ss 12(3), 13(1). The relevant Minister is currently the Attorney-General: Governor-General of the Commonwealth of Australia, *Administrative Arrangements Order* (13 May 2025).

213 *SD Act* s 13. In practice I understand that ART members are asked before they are nominated.

214 *Crimes Act* s 3ZZUP(1). 'Magistrate' includes any magistrate in respect of whose office an annual salary is payable: *Acts Interpretation Act 1901* (Cth) s 16C. A magistrate is a judicial officer who presides over a lower state or territory court, such as the New South Wales Local Court or the Magistrates Court of Victoria.

215 The Minister may, by writing, nominate a person who holds appointment as Deputy President, senior member or general member to ART to issue warrants: *SD Act* s 13(1). There is provision for the functions of the deputy presidents, senior and general members of ART to include 'any other functions conferred' by another Act: *ART Act* ss 194(1)(d), 195(1)(d)–(2)(b).

Table 4 – Number of judges and nominated ART members authorised to issue SLAID Act warrants, 2025

Judges who can issue SLAID Act warrants								
	SA	Qld	ACT	Tas	Vic	NT	WA	NSW
FCFCOA (Div 1)	0	1	1	0	3	0	6	3
FCFCOA (Div 2)	1	7	1	0	3	1	0	11
FCA	1	2	0	0	5	0	2	7
Total judicial officers	2	10	2	0	11	1	8	21

ART Members who can issue SLAID Act warrants								
	SA	Qld	ACT	Tas	Vic	NT	WA	NSW
ART Deputy President	1	1	0	0	2	0	0	2
ART Senior members	5	5	1	1	4	1	1	3
ART General members	1	1	1	2	4	0	3	2
Total ART members	7	7	2	3	10	1	4	7

Note: This information is drawn from the Register of Authorised Persons for Warrants and Other Functions under ss 12 and 13 (respectively) of the *Surveillance Devices Act 2004* (Cth). It is accurate as at 11 March 2025.

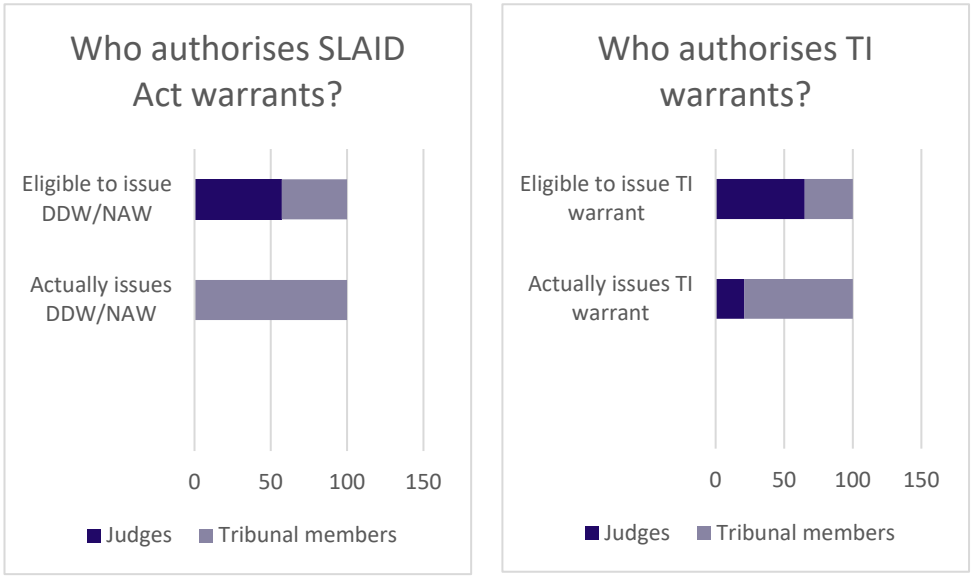
Who actually issues warrants?

7.9 There are more judges appointed to issue *SLAID Act* warrants than there are ART members. However, in practice, all DDWs and NAWs have been issued by a small number of ART members.[216]

> All DDWs and NAWs have been issued by a small number of ART members.

7.10 Applicants choose to go to ART members rather than judges when applying for a warrant. This is consistent with the trend in authorisation of telecommunications interception warrants, which can also be issued by either a nominated judge or ART member. For example, in 2023–24, there were 61 judges and 33 ART members authorised to issue interception warrants, and 79% of interception warrant applications were made to ART members.[217]

Figure 2 – Number of members and judges who authorise SLAID Act and telecommunications interception warrants



216 This review considered warrants from the commencement of the *SLAID Act* to 31 December 2024.

217 This includes a small number of warrants that can only be issued by judges, such as those used by the National Anti-Corruption Commission. In Queensland and Western Australia, significantly more interception warrant applications were made to judges than in other states: AGD, *2023–24 Annual Report under the Telecommunications (Interception and Access) Act 1979 and Part 15 of the Telecommunications Act 1997* (Report, 20 March 2025) 12–13.

Constitutional constraints on issuing authorities

7.11 There are legal and practical constraints on who can issue warrants. The legal constraints arise from the constitutional separation of powers. The practical constraints include issuing authorities having enough time to issue warrants and those authorities being able to do so in a timely way without distracting them from their core work.

7.12 Following the High Court ruling in *Grollo v Palmer*[218] (*Grollo*) many judges indicated that they were no longer willing to issue warrants. This led to a change in legislation to allow members of the then Administrative Appeals Tribunal (AAT) (now ART) to begin issuing warrants.[219]

7.13 There is a great deal of scholarship and nuance in the distinction between Commonwealth judicial and non-judicial power,[220] but the essential point for this review is that the issuing of warrants is considered an administrative function.[221] The practical result is that judges (and magistrates), who exercise federal judicial power, cannot issue warrants in their judicial capacity; they can only issue them in their personal capacity. This is also known as *persona designata*.[222] This puts Australia in quite a different position from other countries that we often compare ourselves to, such as the US, Canada and New Zealand, where judges can and do issue warrants in their judicial capacity. These constitutional constraints do not apply to ART members, as they do not exercise 'judicial power'. However, as the issuing of warrants is not a statutory function of ART, members are described as issuing warrants in their personal capacity.

7.14 The practical consequences of judges, magistrates and ART members acting in their personal capacity to issue warrants are many. The time taken to issue warrants detracts from their ability to undertake their core work. There is also limited scope for centralised management, data collection and allocation of warrant applications; and limited access to relevant training, including about the kinds of technical capabilities associated with warrants such as *SLAID Act* warrants. The decentralised system gives little opportunity for peer-to-peer development or national consistency of approach for these types of warrants.

218 (1995) 184 CLR 348.

219 AGD, *Submission 20,* 9. The ART was established by the *ART Act* and commenced operation on 14 October 2024.

220 For example, it is not possible to precisely define judicial power: *R v Davison* (1954) 90 CLR 353, 366 (Dixon CJ for McTiernan and Fullagar JJ); *Huddart Parker & Co Pty Ltd v Moorhead* (1909) 8 CLR 330, 357 (Griffith CJ). Characterisation as judicial power may involve 'comparison with the historic functions and processes of courts of law': *R v Trade Practices Tribunal; Ex parte Tasmanian Breweries Pty Ltd* (1970) 123 CLR 361, 394 (Windeyer J).

221 *Love v Attorney-General (NSW)* (1990) 169 CLR 307, 321 (Mason CJ; Brennan, Dawson, Toohey and Gaudron JJ) affirmed by *Ousley v The Queen* (1997) 192 CLR 69, 80 (Toohey J), 87 (Gaudron J) 100 (McHugh J), 130 (Gummow J). Cf *R v Tillett; Ex parte Newton* (1969) 14 FLR 101.

222 *R v Kirby; Ex parte Boilermakers' Society of Australia* (1956) 94 CLR 254, 270, 330; *Chu Kheng Lim v Minister for Immigration, Local Government and Ethnic Affairs* (1992) 176 CLR 1, 26. Also see *Hilton v Wells* (1985) 157 CLR 57; *Grollo v Palmer* (1995) 184 CLR 348.

7.15 The fact that warrant issuing is a personal function and not a function of the court is one of the reasons that courts do not provide training and other supports for warrant issuing. The ART does not provide training for personal capacity functions either but does manage a roster and booking system for warrant issuing in larger jurisdictions (for example, Sydney).[223]

> In practice, reliance on 'personal capacity' decision-making means that warrant issuing is a distraction from core functions; and there is limited capacity for centralised management and provision of support.

Warrant issuing needs independence

7.16 In this review there was no dispute that the issuing authority needs to be, and be seen to be, 'independent' (aside from certain time-critical emergency situations (see Chapter 13)). Broadly speaking, independence *includes* having 'the professional experience and cast of mind'[224] and the ability to act impartially and in an unbiased manner. Impartiality may require 'distancing one's self from one's own prejudices and ideology.'[225] The need for the issuing authority to be independent reflects the difficulty of balancing competing public interests in combating serious cyber-enabled and cyber-dependent crime and the intrusiveness of covert electronic surveillance and interference with individual rights.[226]

> There is no dispute that issuing authorities needs to be independent. The key question is: what does 'independent' mean in this context?

7.17 The 'tenure' of both judges and ART members as warrant issuing authorities depends on being authorised for this purpose by the Attorney-General – an

223 ART and INSLM, *Agreed Record of Meeting* (17 March 2025). I am aware that at various points in time individual (then Administrative Appeals Tribunal (AAT)) members have developed their own notes on authorising warrants (mostly telecommunications interception warrants) and have shared this knowledge with tribunal colleagues, at least in their state. This is to be commended, but it is not a substitute for coordinated and ongoing professional development.

224 *Grollo v Palmer* (1995) 184 CLR 348, 368.

225 Chief Justice Susan Kiefel, 'Judicial Independence – From What and to What End?' (Austin Asche Oration, 26 March 2021) 3 cited in Australian Law Reform Commission (ALRC), *Without Fear or Favour: Judicial Impartiality and the Law on Bias* (ALRC Report No 138, December 2021) 66.

226 *Grollo v Palmer* (1995) 184 CLR 348, 368.

authorisation that can be revoked.[227] I heard evidence from several civil society groups and the Australian Human Rights Commission that actual and perceived independence would improve if issuing authorities were restricted to serving or former superior court judges.[228] Some argued that, because ART members do not have the security of tenure of judicial officers and are dependent on the government for reappointment, there is a risk that the perception of independence may be diminished.[229]

7.18 Judicial independence entails a stringent separation of the judicial branch of government from the executive and requires robust protection of security of tenure.[230] It does not necessarily follow that every decision that requires a degree of impartiality must be made by a judge as a member of a constitutionally protected court. ART members are also required to act with independence in the discharge of their statutory administrative review functions and their decisions in that capacity can have real impact on the rights of individuals.[231] ART members may not have the tenure and level of independence of a judicial appointment, but they do operate at arms-length from government and have experience in review of government decisions.

7.19 In my view, the essential elements of 'independence' of an individual issuing authority in the context of issuing police and criminal intelligence warrants are professional experience and cast of mind; the ability to act impartially and in an unbiased manner; and a role that is, and is perceived to be, at arms-length from government – in particular, from the applicant agency. Judges, magistrates and ART members are all capable of falling within this description. Although I acknowledge that the public perception of independence is likely to be higher for magistrates and judges.

> Not every decision that requires a degree of independence must be made by a judge.

227 *SD Act* ss 12–13. A specific revocation provision only applies to nominated ART members (s 13). However, the power to declare a consenting judge to be an issuing authority would be interpreted having regard to s 33(3) of the *Acts Interpretation Act 1901* (Cth).

228 Law Council, *Submission 23*, 33 [111]; Joint Academic Submission, *Submission 15*, 8; AHRC, *Submission 21*, 9 [28] (recommendation 4); QCCL, *Submission 6*, 6; Alliance for Journalists' Freedom (AJF), *Submission 7*, 4 [3.1]; NSWCCL, *Submission 10*, 4 [3.4].

229 While the Law Council acknowledged strengthened provision for merit-based appointment and 5-year terms under the *ART Act*, they reiterated the concern that '[m]embers of the ART lack the security of tenure of judges and remain, ultimately, dependent on the Executive for reappointment': Law Council, *Submission 23*, 32 [106]; NSWCCL, *Submission 10*, 4 [3.2]–[3.4].

230 ALRC, *Without Fear or Favour: Judicial Impartiality and the Law on Bias* (Report No 138, December 2021) 66.

231 A distinguishing feature of the legislation establishing ART (in comparison with the previous AAT enabling legislation) is the entrenchment of independence as a statutory objective: *ART Act* s 9. There is also provision for ART members to take an oath similar to the oath taken by Federal Court judges and associated with judicial independence: *ART Act* s 213. See further, on the implications of these provisions for independence, Justice Emilios Kyrou, 'Inaugural Ceremonial Sitting of the Administrative Review Tribunal' (Speech, Melbourne, 14 October 2024).

7.20 Proper independence in the system of issuing warrants also requires that warrants, like cases, are independently allocated. That is, applicants should have no ability (real or perceived) to select the official who considers a warrant application (and who does not). This is not always currently the case, at least partially because warrant issuing is a personal capacity function. Access to independent technical advice is also required. These issues are discussed further in Chapter 9.

Who should issue warrants?

7.21 As I explained in Chapter 2, the current system for issuing electronic surveillance and *SLAID Act* warrants is based on a much earlier system that was designed at a time when searches were overt, had more limited scope for privacy intrusion and did not involve complex technology. This review provided an opportunity to test whether that system is effective in the modern context of highly intrusive and often covert and technically complex powers that are unlikely to be challenged in a court, such as *SLAID Act* warrants.

7.22 Broadly speaking, 3 potential groups that could issue police and criminal intelligence warrants emerged from submissions and consultation:

- sitting judges and in particular superior court judges
- tribunal members
- retired judges.

7.23 It would be a highly unusual move for any person outside of these categories to issue police and criminal intelligence warrants, and no submissions or proposals to this review suggested that should be the case.

Judges

7.24 As discussed above, currently there are 55 judges of the FCFCOA and FCA who are able to issue *SLAID Act* warrants, although none have actually done so. A similar number of federal judges are authorised to issue other types of warrants, including interception warrants.

Benefits of having judges issue warrants

7.25 Non-government submissions strongly supported the proposal that *SLAID Act* warrants be issued only by judges or former judges. Many said that the ability to issue warrants should be limited to those from superior courts.[232] There were different arguments for why this should be the case, but the themes included public confidence, experience, independence and rigour.

232 The Federal Court of Australia and Division 1 of the FCFCOA (which deals with family law matters) are superior courts.

7.26 The PJCIS recommended that DDWs and NAWs be issued only by superior court judges. One rationale for judicial authorisation was that it would improve public confidence and assurance that the issuing of the warrants and exercise of the powers would be subject to an independent issuing process. [233]

7.27 The Australian Human Rights Commission said that its 'preference for authorisation by superior court judges (retired or serving) for all *SLAID Act* warrants is driven by the need to ensure a sufficiently robust level of scrutiny and accountability for the use of these covert and intrusive powers.' It also said that judges are 'best placed to objectively evaluate whether [*SLAID Act* powers] are necessary, proportionate and justified under the circumstances.'[234]

7.28 The Joint Academic Submission highlighted 'substantial complexity' of the issuing criteria, including 'broad and interlacing definitions'; 'potentially severe (and covert) impacts on rights'; 'the need for robustly independent mindset'; 'a sophisticated appreciation of appropriate levels of deference'; and limited access to judicial review.[235]

7.29 The Law Council of Australia recommended that *SLAID Act* warrants be issued only by judicial officers of state, territory or federal superior courts with criminal trial experience. Their reasons included independence, public confidence and experience in making decisions closely related those involved in warrant issuing.[236] The Joint Academic Submission and the Law Council also highlighted comments from the majority of the High Court in *Grollo*, which emphasised the advantages of the independent disposition, professional experience, and skills of judicial officers in the context of authorising electronic surveillance:

> the professional experience and cast of mind of a Judge is a desirable guarantee that the appropriate balance will be kept between the law enforcement agencies on the one hand and criminal suspects or suspected sources of information about crime on the other. It is an eligible Judge's function of deciding independently of the applicant agency whether an interception warrant should issue that separates the eligible Judge from the executive function of law enforcement. It is the recognition of that independent role that preserves public confidence in the judiciary as an institution.[237]

7.30 The New South Wales Surveillance Devices Commissioner (the NSW SD Commissioner) said that the role of senior judges 'at the centre of the authorisation

---

233 *PJCIS SLAID Report* 131–2 [6.58] Recommendation 9 (the PJCIS also recommended that ATWs be issued by judges). See also the concerns raised by the PJCHR about issuing authorities: PJCHR, *Human Rights Scrutiny Report* (Report No 3 of 2017, 17 March 2021); 85–6 [2.70], 98 [2.103].

234 AHRC, *Submission 21*, 8 [26].

235 Joint Academic Submission, *Submission 15*, 8.

236 Law Council, *Submission 23*, 31–6, Recommendation 10. As an alternative to judicial issuing, the Law Council supported considering authorisation by a specialised part of the ART akin to an investigatory powers division headed by a retired judge of the type proposed by former Monitor James Renwick: Law Council, *Submission 23*, 37–9.

237 *Grollo v Palmer* (1995) 184 CLR 348, 367 [20] (Brennan CJ; Deane, Dawson and Toohey JJ).

process is a key source of public confidence.'[238] The Alliance for Journalists' Freedom said that warrant issuing should be limited to judges 'partly because of the additional skills and experience they bring to the case, but also to improve public confidence that warrants are being issued appropriately.'[239] Similarly, the Australian Human Rights Commission said that having warrants issued only by serving or retired judges 'would enhance public confidence in the fairness and impartiality of the process, reducing the risk of misuse or overreach by law enforcement.'[240]

7.31 The New South Wales Council for Civil Liberties observed:

> a superior court judge would have suitable seniority and the breadth of experience required to be entrusted with the power to issue such intrusive warrants. Further, as tenured officials, there is far less risk that they would appear to the public to lack independence.[241]

7.32 Interestingly, warrants for the National Anti-Corruption Commission (NACC) may only be issued by a superior court judge.[242] When the amendments were made that prevented ART members from issuing NACC warrants, the reason given was:

> The amendments would promote the right to privacy by requiring decisions about the issuing of warrants authorising the use of covert electronic surveillance powers under the *SD Act* and *TIA Act* to the NACC to be made by an eligible Judge of a federal superior court of record … Restricting the power to issue electronic surveillance warrants to the NACC to senior members of the federal judiciary would provide greater assurance that any exercise of the powers authorised by those warrants would meet the statutory criteria for the issue of those warrants.[243]

7.33 There are clearly benefits to having judges, especially superior court judges, issue warrants. This includes the high level of public confidence in this role and the level of experience judicial officers have in making decisions that affect the rights of individuals.[244] Judges (and magistrates) also have experience in robustly testing evidence put forward by police.

There are benefits to having superior court judges issue warrants, including public confidence and the level of experience in weighing decisions that affect the rights of individuals.

238 New South Wales Surveillance Devices Commissioner (NSW SD Commissioner), *Submission 2*, 6; see further *SD Act* s 12(1) (definition of 'judge' means a person who is a Judge of a court created by the Parliament).
239 AJF, *Submission 7*, 4 [3.1].
240 AHRC, *Submission 21*, 8 [26].
241 NSWCCL, *Submission 10*, 4 [3.4].
242 *SD Act* s 12(1)(b).
243 Supplementary Explanatory Memorandum, National Anti-Corruption Commission (Consequential and Transitional Provisions) Bill 2022 (Cth) 3 [6].
244 ALRC found that, at a general level, public confidence in the Australian courts is high: ALRC, *Without Fear or Favour: Judicial Impartiality and the Law on Bias* (Report No 138, December 2021) ch 5.

7.34 There are some significant practical barriers to having sitting judges issue warrants. In view of these constraints, other submitters expressed caution about judicial authorisation and preferred other options.[245]

Barriers to greater reliance on having judges issue warrants

7.35 There are key practical and principled barriers to greater reliance on having sitting judges issue warrants, including the increased time burden and potential conflicts with hearing cases:

- There is a limited number of judges (and especially superior court judges) in the federal judiciary and they have limited time for warrant issuing functions.
- Issuance by serving judges does not address the practical implications of 'personal capacity' appointment.
- If the volume of warrant issuing interfered with judicial functions, there are potential constitutional risks.

Limited number of judges and limited time for warrants

7.36 As judges have not actually issued any *SLAID Act* warrants, these warrants on their own cannot be said to impose an unreasonable burden on judges at the moment. To date, there have been fewer than 20 *SLAID Act* warrants per year (including renewals).[246]

7.37 If all *SLAID Act* warrants and renewals were to be issued by FCA and FCFCOA judges, this could start to be a burden, particularly if many applications for warrants occur in a smaller jurisdiction where there is a limited number of judges who have agreed to issue warrants. This would be exacerbated if FCFCOA Division 2 judges (who are not superior court judges and who make up over half of the currently eligible judges) were excluded. The Australian Capital Territory, for example, has only 2 judges who have nominated to issue *SLAID Act* warrants, and only one of those is a superior court judge. It may be feasible for *SLAID Act* warrants to be issued only by federal judges, particularly if procedures were put in place to limit the burden on small jurisdictions. But this option would also increase the burden on judges.

7.38 If all electronic surveillance warrants were to be issued by federal judges, the burden would be significant. For example, there were 3,023 interception warrant

245 Two academics preferred authorisation by ART, with modifications to better realise the advantages of the United Kingdom Investigatory Powers Commissioner's Office (IPCO) system: Philip Glover, *Submission 8*, 3–4; Brendon Walker-Munro, *Submission 3*, 3–4 (Recommendations 3-4).

246 There was evidence from AFP and ACIC that they are planning to use more *SLAID Act* warrants in future, although technical and cost constraints mean that the growth is unlikely to be dramatic: AFP, *Submission 18,* 4–5 [24]; ACIC, *Submission 17*, 3, 5.

applications in 2023–24, with only 639 of those issued by judges.[247] There were also 648 surveillance device warrant applications and 244 renewals sought and made in 2023–24.[248] It seems unrealistic to expect that judges could find enough time to issue warrants if the number of applications and renewals increased by almost 5-fold.[249] It would be even more unrealistic if over half of the judges who are currently willing to issue warrants were excluded because they are not superior court judges. It is entirely foreseeable that, if the amount of time that judges needed to spend on issuing all electronic surveillance warrants were to increase, it would have a negative impact on the core work of the courts and might contribute to delay in finalising cases as well as delay in issuing warrants.

If all electronic surveillance warrants were to be issued by superior court judges, the burden on judicial time would be significant.

7.39 One way of spreading the workload of issuing warrants would be to make a wider range of judges eligible to issue warrants. The Law Council of Australia suggested that warrants 'could be issued by judicial officers of state, territory and federal superior courts.'[250]

7.40 One difficulty with this approach is that state and territory superior court judges hear most serious criminal matters. It is possible that, because of a risk of apprehended bias, a warrant issuer may be required to recuse themselves from hearing a matter involving an accused who has been the subject of a warrant issued by the judge.[251] The risk of a warrant covering a person who is later charged with a serious criminal offence is particularly significant for NAWs, which can cover a large number of people.[252] There is some risk of this with FCFCOA (Div 2) judges, but they have less matters relating to criminal law.

7.41 A further practical challenge is that, if sitting state and territory judges were to be asked to issue *SLAID Act* and other Commonwealth warrants, there would need to be careful negotiations with each jurisdiction and court. It is not clear that they would be willing to take on this additional workload, even with financial compensation from the Commonwealth.

247 AGD, *2023-24 Annual Report under the Telecommunications (Interception and Access) Act 1979 and Part 15 of the Telecommunications Act 1997* (Report, 20 March 2025) 12-13.

248 *SD Act Annual Report 2023-24*, 11–12, 14. This report does not include details about whether these warrants were issued by judges or ART members.

249 This calculation assumes judges currently authorise a similar proportion of *SD Act* warrant applications as telecommunications interception applications.

250 Lloyd Babb, Law Council, *Public hearing transcript*, 19 February 2025, 43.

251 On actual bias see *Jia v Minister for Immigration and Multicultural Affairs* (1998) 84 FCR 87, 104 (French J), cited with approval in *Minister for Immigration and Multicultural Affairs v Jia* (2001) 205 CLR 507 [35]–[38] (Gleeson CJ and Gummow J). On apprehended bias see *Ebner v Official Trustee in Bankruptcy* (2000) 205 CLR 337, 344 [6] (Gleeson CJ; McHugh, Gummow and Hayne JJ, Callinan J agreeing) cited in *Charisteas v Charisteas* (2021) 273 CLR 289, 296 [11] (Kiefel CJ; Gageler, Keane, Gordon and Gleeson JJ).

252 AGD, *Submission 20*, 9. Limitations on the ability to adduce NAW material in evidence may also result in the prosecutor or defendant claiming that the judge was presented with information about the accused outside of the trial context.

While there may be benefits to using sitting judges from states and territories to issue *SLAID Act* and other warrants, it is unlikely to be a practical option.

Limitations inherent in 'personal capacity' functions would remain

7.42 As discussed earlier, due to the constitutional separation of powers, judges who exercise federal judicial power can only issue warrants in their personal capacity. Courts with federal jurisdiction are cautious about using court resources to support non-judicial functions for the same reason. This means that there is little scope for centralised management, data collection and allocation of warrant applications; and limited access to relevant development opportunities.

7.43 Because the system relies on judges volunteering to issue warrants in addition to their judicial workload, there is little scope for managing the appointment process in a way that prioritises experience in criminal law matters. It is not a requirement of appointment of FCA or FCFCOA judges that they have criminal law expertise.[253]

7.44 Perhaps the biggest limitation with 'personal capacity' work is that it is done on top of an already full judicial workload. AGD highlighted that there is a risk in greater reliance on superior court judges volunteering for appointment. It said this may be 'fundamentally very challenging' in the context of managing judicial workloads alongside the need to maintain 'accessibility to agencies' for prompt warrant issuing. It also said it was concerned that '[an] increase in their workload [would] impact the willingness of judges to take on that role in *persona designata*.'[254]

Possible constitutional issues

7.45 The decision in *Grollo* makes clear that judges who exercise federal judicial power can issue warrants in their personal capacity, but there are some caveats. These caveats include that the conferral of a personal function must not be incompatible with either the judge's performance of their judicial functions or with 'the proper discharge by the judiciary of its responsibilities as an institution exercising judicial power.'[255] AGD said that the things that are likely to increase the risk that issuing warrants would interfere with or be incompatible with judicial functions include:

253 For example, Division 1 of the FCFCOA was established to function as a specialist family law court and it is a requirement for appointment that judges must be suitable persons to deal with family law matters: *Federal Circuit and Family Court of Australia Act 2021* (Cth) s 11(2)(b).

254 Sarah Chidgey, Deputy Secretary, AGD, *Public hearing transcript*, 20 February 2025, 61.

255 *Grollo v Palmer* (1995) 184 CLR 348, 364–5 (Brennan CJ; Deane, Dawson and Toohey JJ).

- the complexity of applications
- whether applications would be likely to divert judges from their judicial responsibilities (for example, if required to be heard during a sitting period or urgently)
- given that *SLAID Act* powers, and in particular NAWs and ATWs, will often relate to a large number of alleged serious criminals, whether any related matter is likely to come before the judge – in particular, for judges vested with a criminal jurisdiction, and
- the aggregate total of in *persona designata* functions performed by those judges.[256]

7.46 As the Attorney-Generals' Department said, 'these considerations may be particularly relevant in jurisdictions with fewer judges, as judges may have a more limited ability to recuse themselves from a matter where they had issued a warrant that is related to the proceeding.'[257]

7.47 Issuing *SLAID Act* warrants alone is unlikely to be problematic for any of these reasons. However, if the system were to expand to all warrants, the risk would increase. It is not necessary to explore that further here because, for the reason already discussed, a system that relies primarily on sitting judges issuing a large numbers of warrants in their personal capacity is not practical.

While there are benefits to using sitting judges to issue *SLAID Act* and other warrants, it is unlikely to be a practical option for a large number of warrants.

Magistrates

7.48 Magistrates are involved in most criminal proceedings at various points in the criminal justice process.[258] They preside over trials for summary offences and certain indictable offences that can be tried summarily.[259] For example, in New South Wales, the Local Court deals with over 90% of all criminal matters in the state.[260] However, magistrates are unlikely to be presiding over trials for the types of serious organised crime that *SLAID Act* warrants are intended to be used for.

7.49 Currently, all magistrates can issue ATWs (but not DDWs or NAWs). Magistrates have long issued warrants to conduct physical searches of premises. This now includes searches of computers found at the premises and data that can be

256 AGD, *Submission 20*, 9.
257 AGD, *Submission 20*, 9.
258 For example, hearing bail applications and conducting committal proceedings to determine whether indictable offences should be committed to be heard in the District Court or Supreme Court.
259 For Commonwealth offences, see *Crimes Act* ss 4H, 4J. The threshold for state matters is defined differently in each state and territory. For example, in New South Wales see *Local Court Act (No 93) 2007* (NSW) s 9(c) and *Criminal Procedure Act (No 209) 1986* (NSW) sch 1. There is legislation establishing the criminal jurisdiction of each magistrate's court: see, for example, *Magistrates Court Act 1930* (ACT) s 19.
260 Local Court of New South Wales, *Annual Review 2023* (Report, 26 June 2024) 7.

accessed from them.[261] When ATWs were introduced, they were placed in the *Crimes Act* and, like search warrants, all magistrates were able to issue them. According to the Revised Explanatory Memorandum, this was for 'consistency with other law enforcement powers in the *Crimes Act*, due to the fact that account takeover warrants will often by applied for at the same time as other warrants in the *Crimes Act*.'[262] This reasoning seems to be based more on convenience than consideration of the potential nature of ATWs. AGD suggested that the ability for magistrates to issue ATWs is akin to physical search warrants that allow for the seizure of digital assets.[263]

Physical search warrants versus ATWs

7.50 While there may be some surface similarities between a physical search warrant and an ATW, I do not agree that they are equivalent. There are important differences which are relevant to the safeguards that are needed for the issuing of warrants. The first is that ATWs can be covert. Search warrants are overt – the person whose premises is being searched will ordinarily be notified of the search and is therefore in a position to challenge the warrant.[264] The fact that there is almost no practical chance of an individual being able to effectively challenge a *SLAID Act* warrant is one of the key reasons that additional safeguards are required in the system for issuing these warrants.

7.51 I acknowledge that some ATWs may be executed in an overt manner – for example, if a person is requested or required to provide their password and this is used to change the password and lock them out of their account. However, this is not the only way ATWs can be used. For example, ACIC gave evidence about plans to use ATWs in a covert manner (see Chapter 5).

7.52 A second reason that ATWs differ from search warrants is that highly sophisticated technology can be used to take over an account, particularly if the takeover is remote and covert. There are risks and nuances in this type of technology that may require independent technical advice (see Chapter 9).

7.53 The system for issuing ATWs cannot be premised on the assumption that police and criminal intelligence agencies will only use overt and low-technology methods. To the contrary: the system should assume that the warrants will be used to their maximum lawful extent – which, in the case of ATWs, includes covert and advanced means. ACIC identified technical complexity and the need to develop new capabilities as reasons they had not yet used any ATWs.[265]

261 *Crimes Act* s 3FA.
262 Revised Explanatory Memorandum 12 [14] (emphasis added).
263 AGD, *Submission 20*, 7–8.
264 There is provision for a delayed notification search warrant for certain terrorism matters. There are very few of these and, in such cases, notification is *delayed*, not absent: *Crimes Act* pt IAAA.
265 ACIC, *Submission 17*, 3.

The system for issuing ATWs cannot be premised on the assumption that police and criminal intelligence agencies will only use overt and low-technology methods.

7.54 Magistrates are not authorised to issue Commonwealth electronic surveillance warrants or warrants under the *TIA Act*, other than stored communications warrants.[266] At the state and territory level, in at least some jurisdictions, magistrates can issue surveillance device warrants – but only the less intrusive tracking device warrants.[267]

Practical challenges in providing additional supports

7.55 This report proposes that the issuing of *SLAID Act* warrants, including ATWs, be supported by PIMs, access to independent technical advice, ongoing professional development and other new safeguards (see Chapters 8 and 9). These are important for existing ATWs and will be even more important as more sophisticated techniques are used and if ATWs are extended to include named person warrants as recommended in Chapter 6. In theory, these supports could be extended to magistrates who issue ATWs, but it is difficult to see how this would work in practice. There are around 550 magistrates across Magistrates Courts and Local Courts in states and territories.[268] Many will never be asked to issue an ATW and others may see these types of warrant applications only very rarely (the highest number of ATWs issued in any year so far is 6). It would be expensive and inefficient to introduce new procedures into every jurisdiction so that magistrates who may be asked to issue an ATW are properly supported. Magistrates Courts are notoriously busy. As discussed later in this chapter, there are alternative options for issuing ATWs. These would not impose any burden on Magistrates Courts.

ATWs require additional safeguards and it would be very difficult to put these in place in Magistrates Courts around Australia.

7.56 One argument for leaving ATWs with magistrates rather than moving ATWs to a new issuing system is that, at least for AFP, ATWs are sometimes sought in conjunction with search warrants, and it would be inefficient for police to have to contact a magistrate and another issuing authority to seek other warrants for the same operation. I note that ATWs may also be sought in conjunction with NAWs or DDWs, which cannot be issued by magistrates. State police face a similar challenge in operations that require authority to use telecommunications interception (generally sought from an ART member) and a state surveillance device (generally from

266 For example, see *TIA Act* s 39 (telecommunications interception warrants), 6DB, 116 (the definition of 'issuing authority' includes magistrates for the purposes of stored communication warrants).

267 See, for example, *Surveillance Devices Act (No 64) 2007* (NSW) s 17(2)(b); *Police Powers and Responsibilities Act 2000* (Qld) s 327(2)(a)(i); *Surveillance Devices Act 1999* (Vic) s 14(2).

268 'Judicial Gender Statistics: Number and Percentage of Women Judges and Magistrates at 30 June 2024', *Australasian Institute of Judicial Administration Incorporated* (Web Page, July 2025).

a Supreme Court judge). For ATWs the solution is to empower the new issuing authority for ATWs to also issue search warrants (and any associated assistance orders) when they are sought together. I see advantages for the issuing authority and PIM in being able to consider all relevant warrants for an operation at the same time wherever possible.

Magistrates should not issue *SLAID Act* warrants.

Administrative Review Tribunal members

7.57 As has already been discussed in this chapter, it takes time to issue a warrant, and that is time that cannot be spent on the core functions of a court or tribunal. This problem is particularly acute for ART because, in practice, ART members issue the vast majority of federal electronic surveillance warrants and *SLAID Act* warrants.

7.58 Several other reasons why ART members should not be asked to issue law enforcement and criminal intelligence warrants arose in this review, including:

- Judges and retired judges are more likely to provide the level of public confidence required for the issuing of highly intrusive warrants such as *SLAID Act* warrants.
- Very few ART members have experience in criminal law and criminal proceedings, nor is such experience necessary for the core work of ART.
- ART has limited oversight of, and provides little support to, members for 'personal capacity' functions and ART's funding model is not structured for these types of functions.

Time taken to issue warrants detracts from core work

7.59 The ART exists to review a range of government administrative decisions in a manner that is 'fair and just' and 'ensures that applications to the Tribunal are resolved as quickly, and with as little formality and expense as a proper consideration of the matters before the Tribunal permits.'[269] Most of the ART's work relates to review of decisions about visas, including migration and refugee visas; Centrelink payments; the National Disability Insurance Scheme; taxation; child support; workers compensation; and veterans' entitlements.[270] ART members are selected and engaged to review administrative decisions of these types and the

269 *ART Act* s 9(a)–(b).

270 In 2023–24, 81% of the applications lodged were in the Migration and Refugee and Social Services and Child Support Divisions: AAT, *Annual Report 2023–24* (Report, 24 September 2024) ch 3.

selection criteria do not reference 'personal capacity' functions such as warrant issuing.[271]

7.60 I received advice from the President and Principal Registrar on behalf of the ART that warrant issuing is a 'significant distraction' from the core work of the ART, which is reviewing administrative decisions. Specifically, 'time spent issuing warrants detracts from the ability of the ART to manage its actual caseload and contributes to a growing backlog of cases.' The ART has an increasing caseload and, while funding is 'demand driven,' this relates only to its core work of reviewing administrative decisions and it does not guarantee that an individual member's time will be available when required for cases or warrants.[272]

> Time spent issuing warrants detracts from the ART's ability to manage its core workload and is contributing to a growing backlog of cases.

7.61 This review sought to identify exactly how much time on average is currently given to considering the content of warrant applications.[273] In 2023–24, members of the then AAT considered warrants and other 'personal capacity' applications on 2,192 'occasions' and 268 were out-of-hours appointments.[274] The ART has data for some jurisdictions, but it is recorded as time spent in 'sessions' for personal capacity functions. A session might include an unrecorded number of applications and there might also be administrative time in setting up appointments; and warrants are not separated from other personal capacity functions. Therefore, it was not possible to establish how long is spent considering 'average' warrant applications. In any case, caution would be needed with this statistic, as *SLAID Act* warrants, which make up a small fraction of all warrants, are likely to be more complex than 'average warrants.' Whatever the exact amount of time is, I accept the evidence from the ART that it is having a significant and negative effect on the core work of the Tribunal.

271 Selection criteria for non-judicial deputy presidents, senior members and general members includes 'decision-making and reasoning skills' and 'ability to conduct hearings and other Tribunal case events' and 'writing and communication skills': *Administrative Review Tribunal Regulations 2024* (Cth) s 15.

272 ART and INSLM, *Agreed Record of Meeting* (17 March 2025) 2.

273 In 2019, AAT indicated that the average duration of an appointment relating to warrant applications under the *SD Act* was 24 minutes, and the shortest amount of time was one minute. AAT, *LCC-SBE19-164 – Warrants under the Surveillance Devices Act 2004 Issued by the AAT*, Response to Question on Notice, Budget Estimates 2019–20, Senate Legal and Constitutional Affairs Committee (22 October 2019) 5.

274 AAT, *Annual Report 2023-24* (Report, 24 September 2024) ch 2. This figure includes all applications relating to warrants, controlled applications and other non-tribunal functions. Multiple warrants or other applications may be considered in each 'occasion.'

Public perception of Administrative Review Tribunal member suitability as compared to judges

7.62 As discussed earlier in this chapter, my view is that ART members have sufficient independence for the task of issuing warrants. I also have no reason to doubt that ART members approach the task of issuing warrants with care and diligence. There are some members who have issued telecommunications interception and surveillance devices warrants for a long time. A slightly different question is whether the public perceives them as having the same level of expertise, gravitas and independence as judges to play the critical role of being the primary decision-maker in the exercise of invasive law enforcement or criminal intelligence powers.

7.63 Public confidence in those who issue warrants is important but difficult to measure. As discussed above, evidence to this review strongly suggests that current or retired judges (and especially superior court judges) are perceived as the *most* independent and *best* positioned to scrutinise and challenge warrant applications put before them.

Lack of criminal law experience

7.64 ART member expertise is naturally focused on administrative review. One of the areas that may undermine public confidence in the system for issuing criminal warrants is whether ART members have expertise and experience in the criminal justice system. This does not arise for ART decisions made in areas of specialty for the Tribunal, such as review of migration, social security and child support matters.

Is experience in criminal law necessary to issue criminal warrants?

7.65 The Law Council of Australia said that the 'adjudicative skills' of state, territory and Commonwealth judicial officers with 'recent experience in criminal trials are well-adapted to the factual and legal complexities that are likely to arise in electronic surveillance warrant applications.'[275] They said this is because, to prevent the risk of a retrial, trial judges must pre-empt issues of unfairness, including in relation to the rules of evidence, even if the defence does not object.[276] This is analogous to the covert warrant issuing context, where the subject of the warrant does not have the opportunity to make submissions. The Law Council also said that '[k]nowledge of comparative cases, which is applied by a trial judge in sentencing, may be of particular assistance in scrutinising the issuing threshold' and weighing the gravity

275 Law Council, *Submission 23*, 34 [113]. Some civil society submissions expressed agreement with that point: Karen Percy, Media Federal President, Media Entertainment and Arts Alliance (MEAA), *Public hearing transcript*, 19 February 2025, 22.

276 For example, a criminal trial judge must be 'alert to problems with the prosecution's evidence even if the defence does not object' and they 'must ensure that the accused has a fair trial without unnecessarily hindering the prosecution in the presentation of its case': Law Council, *Submission 23*, 34 [114], citing Justice Susan Kiefel, 'On Being a Judge' (Speech, Chinese University of Hong Kong, 15 January 2013) 6.

of the conduct alleged in a warrant application.[277] The Victorian PIM underlined the importance of familiarity with the criminal justice system from investigation by law enforcement agencies through to trial, including a broad understanding of the admissibility and inadmissibility of evidence.[278] The ART also observed that experience in criminal law would be valuable for warrant issuing.[279]

7.66 The selection criteria for judicial commissioners who authorise warrants in the United Kingdom describes experience in public law as essential and recent experience of the criminal law and criminal proceedings involving those involved in serious and organised crime as *useful* but not essential.[280] In the United Kingdom, judicial commissioners approve intelligence warrants, including those used by Government Communications Headquarters, and there are strict limits on the use of telecommunications interception material in evidence compared with Australia. This may make criminal law experience slightly less relevant in the United Kingdom than in the context of police warrants in Australia. I would say that in the Australian context, including for *SLAID Act* warrants, experience in criminal law and criminal proceedings is *highly desirable* but not essential.

> Experience in criminal law and criminal proceedings is *highly desirable* but not essential.

Would increased funding for the ART resolve concerns?

7.67 I asked the ART whether the issue is primarily one of funding and whether increasing funding to account for 'personal capacity' matters would resolve their concerns. The ART advised that it would not:

> All of the concerns above would continue to apply, even if significant extra funding was provided to appoint additional Members and provide a dedicated national secretariat. Such a model would not resolve the fundamental issue that issuing warrants is not an administrative review function for which Members are selected and trained and that this work detracts from the core work of the Tribunal whose administrative review caseload is expected to continue to increase.[281]

7.68 I also explored whether creation of a specialised 'list' might be a mechanism for selecting members with expertise relevant to issue criminal warrants and whether there may be overlap with the skills required for review of ASIO decisions.[282] The

277 Law Council, *Submission 23*, 35 [117].
278 Public Interest Monitor – Victoria (Victorian PIM), *Submission 24*, 8.
279 ART and INSLM, *Agreed Record of Meeting* (17 March 2025) 2.
280 Home Office (United Kingdom), *Terms of Appointment for a Judicial Commissioner Appointed Under Section 227(1) of the Investigatory Powers Act 2016* (Document, October 2022) 2.
281 ART and INSLM, *Agreed Record of Meeting* (17 March 2025) 2.
282 A small number of ASIO decisions are reviewable by ART: *ASIO Act* ss 37, 54(1), 83B. The idea of a specialised division of the (then) AAT for issuing certain law enforcement and intelligence authorities was proposed by a former Monitor: James Renwick, former Independent National Security Legislation Monitor, *Trust but Verify: A Report Concerning the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 and Related Matters* (Report, 9 July 2020) sch 1. The proposal was not accepted by government at the time.

ART noted that:

- There is no opportunity to gain criminal law experience as part of the work of the ART. It may be that review of ASIO decisions has some overlap with the types of issues relevant to warrants, but there are very few of these cases each year (3–4) and they are handled by the President and deputy presidents, not the members and senior members who issue most warrants.
- Creating a 'list' of this type would require legislative amendment and a change to the structure of the ART at a time when the tribunal is still settling into its new legislation and structure.

The ART's concerns about members issuing warrants would not be resolved by funding.

Would making warrant issuing a core ART function resolve concerns?

7.69 As discussed above, there are compelling reasons that ART members should not be asked to issue law enforcement and criminal intelligence warrants in their personal capacity. It was clear from consultations that the ART strongly supports moving to a model where ART members do *not* have a role in issuing warrants.[283] This reflects a focus on delivering the core work of the tribunal: reviewing a range of government administrative decisions in a manner that is fair, just and timely.

7.70 Nevertheless, there are some attractions in utilising the ART to issue warrants, primarily that it is an existing body and has a national footprint; and some of its members have experience in issuing warrants. Therefore, I considered whether increased funding in addition to making changes to the *Administrative Review Tribunal Act 2024* (Cth) (*ART Act*) to make warrant issuing a 'core' ART function would resolve at least the concerns about workload and criminal law experience, noting it is unlikely to change public perception.[284]

7.71 The changes to ART that would be required to make warrant issuing a 'core' function would be significant and would alter the ART model, legislation and potentially membership at a time when ART has just been through a major transformation. It would be challenging to recruit new members based on the attributes needed for warrant issuing including criminal law experience as well as those needed for specialist administrative review. Increasing the size of the membership of the tribunal may ease some of the current pressure caused by time taken to issue warrants, but there is a real risk that the additional time will end up being absorbed by administrative review work and managing the existing backlog of cases. Additional training and administrative support could be provided, but it

283 ART and INSLM, *Agreed Record of Meeting* (17 March 2025).

284 The constitutional issues discussed in this chapter do not apply to ART. This means that warrant issuing could be made a statutory function under the *ART Act*.

is unlikely to be more efficient than the alternative model of using retired judges (discussed below).

7.72 Making the issuing of police and criminal intelligence warrants (that is, administrative decision-*making*) a statutory function of the ART would not sit comfortably with the role of ART as a body responsible for external merits *review* of government administrative decisions.[285] It is also notable that, while issuing warrants is an administrative decision, like other police powers it is not one that the ART can review – a position which appears to be based at least in part on special nature of law enforcement powers. It is difficult to reconcile this with the ART (in contrast to individual ART members) having a statutory function of issuing warrants. There are other government bodies including AGD with a national footprint.

Findings about ART members issuing warrants

7.73 There are compelling reasons why ART members should not continue to be asked to issue law enforcement and criminal intelligence warrants in their personal capacity including detraction from core ART work, public perception and criminal law experience. These issues are unlikely to be addressed through increased funding to ART or making warrant issuing a core ART function.

7.74 The need for the highest possible level of public confidence is perhaps greatest for the most invasive and novel warrants, although confidence in the entire system is needed for authorising invasive powers. *SLAID Act* warrants are particularly invasive and novel. Like NACC warrants, it is important to provide a high level of assurance that the statutory criteria have been satisfied. Public confidence in the use of highly invasive and covert powers for law enforcement and criminal intelligence purposes is best supported by having judges or retired judges issue warrants. Limiting warrant issuing to the President and those deputy presidents of the ART who have judicial experience would be entirely impractical. For the reasons discussed later in this chapter, there is a feasible alternative option for using retired judges to issue warrants.

7.75 I have considered the fact that *SLAID Act* warrants make up only a small fraction of the overall number of warrants issued by ART members. For the reasons discussed elsewhere, the deficiencies in the current *system* for issuing *SLAID Act* warrants apply to other warrant types currently issued by ART, including computer access and interception warrants. My recommendations are necessarily limited to *SLAID Act* warrants, but they should be considered in the broader context of the ongoing review of electronic surveillance powers.

285 *ART Act* s 9. Justice Kyrou has said that 'independence from administrative decision-makers has been a primary consideration in the policy documents that have underpinned the establishment of ART. It is also reflected in the statutory objective of ART in section 9 of the *ART Act*. That section requires ART to pursue the objective of providing an independent mechanism of review': Justice Emilios Kyrou, 'Inaugural Ceremonial Sitting of the Administrative Review Tribunal' (Speech, Melbourne, 14 October 2024).

Given the role of ART, its members are not best placed to provide effective scrutiny of covert surveillance warrants in their personal capacity. The changes that would be needed to make warrant issuing a 'core' function of ART would be substantial and could not resolve all concerns.

7.76 This conclusion does not imply any lack of diligence on the part of any ART members who have issued *SLAID Act* warrants. ART members who issue *SLAID Act* warrants do so on top of their already busy schedules, and I have no reason to doubt their diligence or that they make all reasonable efforts to make the current system work.

Retired judges

7.77 An option for enlisting people with substantial judicial experience, including expertise in criminal matters, without burdening the work of courts or the ART is to use retired judges.

United Kingdom uses retired judges

7.78 In the United Kingdom, senior serving and retired judges are eligible to be appointed as judicial commissioners. Judicial commissioners scrutinise warrant applications.[286] In practice, all current judicial commissioners are retired judges. The key advantages to utilising retired judges to issue warrants in Australia are:

- access to a pool of individuals with relevant expertise and gravitas
- no risk of constitutional issues or conflict with future criminal proceedings
- no burden on ART or courts.

7.79 In the United Kingdom, the pool of those eligible to be judicial commissioner is quite limited. It includes only those who have held 'high judicial office' – that is, in the Supreme Court of the United Kingdom, the Court of Appeal in England and Wales, the High Court in England and Wales, the Court of Session, the Court of Appeal in Northern Ireland or the High Court in Northern Ireland; or a person who has held office as a Lord of Appeal in Ordinary.[287]

286 The United Kingdom has a 'double lock' system for relevant warrants – authorities 'submit applications for the use of investigatory powers to a secretary of state or a senior officer; this decision is then reviewed and authorised' by a judicial commissioner prior to the issuing of the warrant: Investigatory Powers Commissioner (UK), *Annual Report of the Investigatory Powers Commissioner 2023* (Report, 20 December 2024) 106.

287 *Investigatory Powers Act 2016* (UK) s 227(2); *Constitutional Reform Act 2005* (UK) s 60(2)(a).

7.80 There are presently 15 judicial commissioners (including the Investigatory Powers Commissioner) who between them manage around 9,500 warrants per year as well as review of around 3,200 targeting decisions.[288] For context the total number of Commonwealth law enforcement and criminal intelligence warrants and renewals in Australia each year is around 4,000.

7.81 Experience suggests that there is benefit in having a single senior retired judge identified as the head. In the United Kingdom this is the Investigatory Powers Commissioner. Their role may include providing guidance (including published guidance) and being involved in recruitment processes, publicly explaining the role of issuing authorities and considering warrants (especially novel or complex matters).

How many retired judges would be needed?

7.82 The number of retired judges required to issue warrants in Australia will depend both on the number of warrants to be covered by the scheme and geographic dispersal as well as the number of warrants that can be managed remotely through a secure platform rather than in person in a capital city with secure facilities.[289]

7.83 Consistent with the submissions from the Law Council of Australia and Dr Glover, a wider pool of potential appointees would be appropriate and might include judges who have retired from the:

- FCA
- FCFCOA (Division 1 and Division 2)
- state Supreme Courts
- state District Courts.[290]

7.84 This review did not survey recently retired judges to assess how many may be interested. But anecdotal comments and the United Kingdom experience, as well as the proposed larger pool of courts to draw from in Australia, suggest that there should not be an issue in finding recently retired judges willing to serve in this capacity. Because individuals would no longer be serving judges, it would not be

288 Email from IPCO office to INSLM, 25 July 2025. Judicial commissioners are expected to work up to 90 days per year considering authorisations for the use of covert powers and in supporting oversight functions of IPCO.

289 I was advised that, since COVID-19, in New South Wales, Victoria and Queensland most police warrants are now managed through a secure online platform. Other jurisdictions were not asked about this in this review.

290 Dr Glover reasoned that 'interested onlookers are less concerned about the appointees' judicial seniority than their *expertise* in the area, as the question of proportionality turns on an understanding of the technical implications of the conduct proposed': Philip Glover, *Submission 8*, 4 (emphasis in original). The Law Council suggested 'there may be benefit in dispersing decision-making across state, territory and Federal Courts to address the risk of perceived executive capture': Law Council, *Submission 23*, 36 [124].

necessary to negotiate with states about their availability.[291]

7.85 The NSW SD Commissioner suggested that a downside of using a dedicated warrant-issuing body rather than current judicial officers is that judicial officers who are 'routinely making determinations on a broad range of issues are more likely to maintain a healthy "judicial edge" and less likely to fall into the "tunnel vision" that can sometimes afflict officers who consistently make determinations within a confined area.'[292] In a different context there has been similar concern about establishing a 'national security court' because of a risk that it would 'inevitably over time give rise to perceptions of capture of judges by executive government.'[293]

7.86 This is a consideration, but I believe that there will be less reason for concern in the proposed new system, which includes a pool of retired judges as well as PIMs, than there is with the current practice of most *SLAID Act* warrants being taken to a small number of ART members. As the Law Council of Australia said, in the context of jurisdiction like the Australian Capital Territory, where there are 2 ART members who can issue warrants, 'there is a real risk that public confidence in the independence and rigour of the warrant authorisation process will be undermined.'[294]

7.87 Details such as whether issuing authorities should be engaged for a set number of full-time days per year (as they are in the United Kingdom) or would be available on a part-time roster will depend on how many warrants are to be issued by this system. Clearly the system would be most efficient if it applied to all electronic surveillance warrants as well as *SLAID Act* warrants, as a minimum number of appointees will be necessary just for *SLAID Act* warrants to ensure availability and that decisions are not concentrated in too small a cohort.

7.88 To provide some security of appointment, a fixed term for issuing authorities (for example, 3 years), renewable once or twice, would be appropriate.[295] If an insufficient number of suitable retired judges can be found, it may be necessary to make provision for other suitably qualified individuals to be appointed. Suitable individuals might include some sitting judges or retired ART members with relevant experience. But the issuing authorities should primarily be retired judges.

7.89 In my view, a system that relies on retired judges to issue warrants strikes the best balance between having warrants scrutinised by those with relevant experience and ensuring public confidence while also avoiding overburdening institutions that have a different core function. If this is not accepted then the alternative would be to have sitting FCA and FCFCOA issue *SLAID Act* warrants with the additional supports discussed in Chapters 8 and 9. Although this would not be feasible for all electronic

291 It is noted that the mandatory retirement age for judges who exercise federal judicial power is 70. Arrangements would need to be made in relation to remuneration and its effect on judicial pensions.

292 NSW SD Commissioner, *Submission 2*, 6.

293 See further Law Council, *Submission 23*, 39 [136] citing Grant Donaldson, former Independent National Security Legislation Monitor, *Review into the Operation and Effectiveness of the National Security Information (Criminal and Civil Proceedings) Act 2004* (Report, 30 October 2023) 122 [450].

294 Law Council, *Submission 23*, 32 [107].

295 Judicial commissioners are appointed for a term of 3 years and may be reappointed upon ceasing to be a judicial commissioner (unless removed from office due to bankruptcy, imprisonment etc): *Investigatory Powers Act 2016* (UK) s 228.

surveillance warrants it should be manageable for *SLAID Act* warrants provided their volume remains low.

Recommendation 6: The issuing authorities should be retired judges. If this is not accepted then it should be current judges for all *SLAID Act* warrants. In either case they must be supported by PIMs and technical advisors.

7.90 Appointing retired judges to issue warrants would be an improvement on the current system, but on its own is not sufficient. Appropriate supporting mechanisms are also needed, at a minimum this should include, PIMs, independent technical advisors and independent allocation of warrants.

Selecting and appointing issuing authorities

7.91 The current process for appointing an eligible judge or ART member to issue warrants, including NAWs and DDWs, is that individuals are asked whether they will consent to being appointed in their personal capacity to issue a range of warrants (usually when they are first appointed to the ART or relevant court) and, if so, the Attorney-General authorises them to grant warrants.[296] While ART members must meet certain minimum qualification requirements,[297] there do not appear to be any specific criteria or any role for the President of the ART or head of the relevant court in this process.

7.92 This can be contrasted with the publicly advertised role description and terms of appointment for IPCO judicial commissioners, which includes specific experience and qualities that are required or 'useful' for appointment to the role and where there is a process for advice to the relevant Minister on appointments.

296 *SD Act* ss 12, 13; *TIA Act* s 6D, sch 1 s 14. All magistrates are automatically authorised to issue ATWs: *Crimes Act* s 3ZZUN.

297 In most cases this requires that the person have been enrolled as a legal practitioner for not less than 5 years: *SD Act* s 13(2).

7.93 The advertised criteria include:

- recent practical experience of public law (essential); recent experience of the criminal law and criminal proceedings involving those involved in serious and organised crime (useful but not essential)
- ability to develop familiarity with the workings and practices of the security and intelligence agencies, law enforcement and other public authorities, including central and local government bodies
- basic IT skills, together with an ability to understand new and existing communication technologies
- knowledge of the supporting legislation (relevant United Kingdom laws listed) (helpful but not essential on appointment)
- ability to analyse situations quickly and in depth
- ability to make sound assessments of facts, priorities and possibilities. [298]

7.94 Additional criteria relating to communication and interpersonal skills and motivation are also listed. All of these criteria seem applicable to the issuing of *SLAID Act* warrants, although, as discussed earlier, I would rate experience in criminal law and criminal proceedings as 'highly desirable.'

7.95 Moving to a model of using retired judges provide opportunity for greater transparency in the criteria for appointment and a defined role for providing advice on suitability to the Attorney-General. The United Kingdom system provides a good model. Noting the earlier finding regarding criminal law experience, the criteria should include that experience in criminal law and criminal proceedings is highly desirable.

> There should be greater transparency in the criteria for appointment and a defined role for providing advice on suitability to the Attorney-General prior to a person being appointed as an issuing authority.

7.96 I have made this a strong suggestion rather than a formal recommendation in recognition of the fact that the core point is that retired judges (or if that is not accepted, then judges) should be the issuing authorities and that the exact mechanics of appointment is a matter that will need to be worked through by the department in consultation with the Attorney-General. I note that the *ART Act* provides a recent model for merit-based appointments.[299]

298 Home Office (United Kingdom), *Terms of Appointment for a Judicial Commissioner Appointed Under Section 227(1) of the Investigatory Powers Act 2016* (Document, October 2022). Appointment by the Prime Minister is based on a joint recommendation by the Investigatory Powers Commissioner, the Lord Chancellor, the Lord Chief Justice of England and Wales, the Lord Chief Justice of Northern Ireland, and the Lord President of the Court of Session.

299 *ART Act* ss 205-209.

Ongoing professional development

7.97 In addition to the skills, knowledge and experience relevant to appointment as an issuing authority, there are matters specific to particular warrants and/or which may need to be the subject of ongoing professional development.

7.98 As noted earlier, I was advised that the ART and courts do not provide training on personal capacity functions, including *SLAID Act* warrants. In contrast, judicial commissioners in the United Kingdom receive induction training and are expected to attend learning and development events which are organised quarterly and on an ad hoc basis (for example, as part of the implementation of new legislation).[300]

7.99 Access to continuing education is important in ensuring that issuing authorities have the expertise and knowledge to understand the technology underpinning warrant applications; and less onerous alternatives and feasible conditions that might be imposed to improve the proportionality of the activities authorised under a warrant. That ongoing education might come from a mix of sources, including police and intelligence agencies, independent technical advisors, oversight bodies and other experts.[301] Particularly for complex warrants like *SLAID Act* warrants, there would also be benefit in providing issuing authorities with the opportunity to periodically meet and discuss their approach to warrants and conditions to promote consistency across the country.

300 IPCO, *Judicial Commissioner Role Description* (Document, 2025) 2. Commissioners are expected to work up to 90 days per year considering authorisations for the use of covert powers and in supporting oversight functions of IPCO. Also see references to the provision of 'extensive training' to judicial commissioners in 'Authorisations', *IPCO* (Web Page, July 2025).

301 The submission from the Victorian Principal PIM highlighted additional suggested areas for professional development and how it should be approached: Victorian PIM, *Submission 24*, 7–8.

Chapter 8: Public interest monitors

8.1 Having concluded that *SLAID Act* warrants should be issued by retired judges, the next question is what other changes are needed to ensure that identified deficiencies in the current system are addressed. A key proposal in this regard is the introduction of Commonwealth PIMs.

8.2 This report uses the term 'public interest monitors' because that is the term used for similar roles that currently exist in Queensland and Victoria. New South Wales has a Surveillance Devices Commissioner. The role of PIMs as proposed by this review draws on the experience of each of these jurisdictions, although the role is not identical to any of them. A different name could be used, but the role of the proposed PIMs is essential. This chapter finds that PIMs should be introduced to:

- support the provision of **complete and accurate information** to issuing authorities by:
  - providing submissions on matters of public interest
  - drawing feedback from oversight bodies to attention
  - assisting to identify situations where independent technical advice may be required
  - highlighting any inconsistencies with earlier applications or reports
- improve the **efficiency** of the system, including by:
  - providing feedback on draft warrant applications
  - contributing to the development of templates and procedures relating to warrants
- help to increase **public and industry confidence** in the system for issuing warrants, including by reporting publicly on their work.

Should a Commonwealth PIM be established?

8.3 There is strong evidence that the operation of similar schemes in Queensland, New South Wales and Victoria has improved the quality of warrant applications, provided substantial assistance to issuing authorities by highlighting key issues in complex application material and enhanced community trust in surveillance devices and telecommunications interception warrants in those jurisdictions. Over time, state PIMs and the NSW SD Commissioner have also improved the warrant application processes, including through greater standardisation of warrant application templates and issuing guidance to warrant applicants. This has led to efficiencies in the system.

Submissions to this review

8.4 Several civil society groups and the Australian Human Rights Commission strongly supported establishing a PIM to review all *SLAID Act* warrants because this would improve the proportionality of the *SLAID Act* scheme and assist in protecting human rights and other public interests.[302]

8.5 For example, the Human Rights Law Centre considered that 'there are viable indications that PIMs both objectively and subjectively improve the quality and exactness of the issuing system, and better align the Warrant regime with the principle of proportionality.'[303] The New South Wales Council for Civil Liberties said that, if *SLAID Act* warrants were to remain, 'it is vital' that a PIM be established to oversee each warrant application and to protect the public interest; and noted the positive impact of the NSW SD Commissioner in NSW.[304] The Australian Human Rights Commission highlighted the utility of a PIM in providing pre-application review and also because they can act as a contradictor. There is also scope for PIMs to improve alignment with Australia's human rights obligations.[305] The Law Council of Australia supported introducing PIMs as a mechanism to 'assist the decision maker to review the information contained in a warrant application more thoroughly, and from more than one perspective.'[306]

Civil society and law groups strongly support introduction of Commonwealth PIMs.

8.6 Some submissions queried the need for a PIM in addition to the role of the independent issuing authority. Dr Glover noted that he had trust in judicial officers (suitably trained and technically literate) to monitor the public interest and to act as 'contestors.' AFP also said that:

> this role would appear to be a duplication of the role of the independent issuing authority who are well placed to consider matters of public interest which are already incorporated into the legal thresholds for the warrants.
>
> Before adopting a PIM model there would need to be careful consideration of the risks of undermining the purposes of the SLAID Act powers, and delaying investigations by introducing additional processes.[307]

302 Human Rights Law Centre (HRLC), *Submission 5*, 8 (Recommendation 1); QCCL, *Submission 6*, 7; AJF, *Submission 7*, 4 [3.2]; NSWCCL, *Submission 10*, 5–6; Joint Academic Submission, *Submission 15*, 9 (Recommendation 3(b)); Internet Association of Australia (IAA), *Submission 16*, 2; AHRC, *Submission 21*, 10 (Recommendation 5); Law Council, *Submission 23*, 58–60 (Recommendations 37–39).
303 HRLC, *Submission 5*, 8 [4.1].
304 NSWCCL, *Submission 10*, 5 [4.1].
305 Lorraine Finlay, Commissioner, AHRC, *Public hearing transcript*, 19 February 2025, 16.
306 Law Council, *Submission 23*, 58 [220].
307 AFP, *Submission 18*, 11 [63].

8.7 Highlighting the public interest in ensuring that warrant applications are considered in a timely fashion, AGD noted that 'the *ex parte* nature of warrant applications … facilitates timely decision making, balanced by clear obligations on agencies to provide issuing authorities with all relevant information.'[308]

> Some government agencies were worried a PIM may delay approval of warrants.

8.8 AGD also considered that any addition of a PIM at the Commonwealth level should be considered as part of broader electronic surveillance reform, noting the importance of retaining a consistent approach for all electronic surveillance powers.[309]

Experience of Queensland, Victoria and New South Wales

8.9 Queensland and Victoria have a system that enables independent PIMs to be heard on warrants for telephone interception warrants and state surveillance device applications.[310] New South Wales has a similar system for state surveillance device warrants but not interception warrants.[311]

8.10 The PIM system has been operating in Queensland since 1997, and in Victoria since 2011. The NSW SD Commissioner was appointed in 2019. These are well established and tested roles. The introduction of the NSW SD Commissioner followed a damning report investigating conduct of officers of New South Wales law enforcement agencies (mainly between 1999 and 2002) by then Acting NSW Ombudsman, Professor John McMillan AO. [312] Similarly, in Victoria PIMs were originally introduced following a 2011 report by the Victorian Ombudsman identifying the need for strengthened scrutiny of the way telecommunications interception warrants were issued.[313] The office of PIM in Queensland was

308 AGD, *Submission 20*, 12.
309 AGD, *Submission 20*, 12.
310 *Police Powers and Responsibilities Act 1997* (Qld)*; Public Interest Monitor Act 2011* (Vic).
311 The Attorney-General (New South Wales) has delegated their functions under pt 3 of the *Surveillance Devices Act 2007* (NSW) to the New South Wales SD Commissioner.
312 Acting NSW Ombudsman, *Operation Prospect: A Special Report to Parliament under s 31 of the Ombudsman Act 1974 and s 161 of the Police Act 1990* (Report, December 2016) vol 5, 765 (Recommendations 25–27) (*Operation Prospect Report*). The Acting NSW Ombudsman recommended that a PIM scheme for both surveillance devices and telecommunications interception warrants be established in New South Wales to address vulnerabilities in approval procedures for these warrants.
313 Victorian Ombudsman, *Investigation into the Office of Police Integrity's Handling of a Complaint* (Report, October 2011) 10 [39], 11 [43]. That report was cited in the Minister's second reading speech: Victoria, *Parliamentary Debates*, Legislative Assembly, 25 October 2011, 4833 (Andrew McIntosh).

introduced to address, among other issues, limited mechanisms to challenge surveillance warrants in a covert context.[314]

New South Wales, Queensland and Victoria have well established PIM or PIM-like roles. They review draft applications and can make submissions about public interest matters.

8.11 While each state has a different approach, the state PIMs and the NSW SD Commissioner broadly have 2 roles:

- **Pre-application review**: In their pre-application review of draft warrant applications, PIMs and the NSW SD Commissioner test the content and sufficiency of the information that the warrant applicant provides – for example, by highlighting 'failures to comply with the requirements of the legislation,' 'confusion or inconsistency,' 'insufficiency of information/evidence in relation to key aspects of the application,' 'inadequacies in the information/evidence relied on and/or its presentation' and 'emerging public interest considerations.'[315] During pre-application review there can be a focus on 'whether in the circumstances of the particular case, does the public's interest in privacy or the public's interest in the detection and prosecution of serious criminal offences prevail?' They also consider matters such as whether the number and type of authorities using different surveillance devices is justified.[316] Pre-application review allows agencies to rectify any agreed deficiencies or strengthen their case before the issuing authority considers the warrant.
- **Submissions**: The Victorian PIM makes submissions to the issuing authority about whether an application should be refused or conditions imposed on the warrant in circumstances where concerns they have raised in the pre-application review stage have not been addressed which should be drawn to the issuing authority's attention.[317] The Queensland PIM described their submissions as fulfilling a 'contradictor role' and routinely addressing human rights considerations.[318] The NSW SD Commissioner said that the role of a public interest advocate may include making submissions to the issuing authority that 'highlight key issues in complex application material,' 'guide the judicial officer around complex legal and factual issues' and 'guard the public interest.'[319]

314 Explanatory Note, Police Powers and Responsibilities Bill 2000 (Qld) 2–3.
315 NSW SD Commissioner, *Submission 2*, 8. See also, Victorian PIM, *Submission 24*, 2–3.
316 Public Interest Monitor – Queensland (Qld PIM), *Submission 13*, 3.
317 Victorian PIM, *Submission 24*, 6.
318 Qld PIM, *Submission 13*, 3. Most often, the right to privacy: Public Interest Monitor (Qld), *Annual Report 2023-2024* (Report, 30 September 2024) 7.
319 NSW SD Commissioner, *Submission 2*, 8.

8.12 The state PIMs and NSW SD Commissioner are remarkably efficient. Each varies their approach to suit the requirements of the state they are in. For example, in New South Wales in 2023–2024, the NSW SD Commissioner consulted with applicant agencies on 33% of applications and made submissions in 12% of all applications for warrants, extensions or variations.[320] Of the applications subject to consultation with warrant applicants, 90% culminated in further development of the application. In contrast, in Queensland a PIM made written submissions in all surveillance device warrant and covert search warrant applications.[321] Victoria sits somewhere between.[322] All have adapted to changes in warrant processes driven in part by COVID-19. For example, most warrants are managed through a secure online platform and most appearances are by phone or an online audiovisual application.

Evidence on the value of state PIMs and NSW SD Commissioner

8.13 I received considerable evidence about the benefit of independent PIMs in Queensland and Victoria and the NSW SD Commissioner. This evidence is consistent with earlier reviews and judicial comments. For example, in 2016 the Acting NSW Ombudsman noted that, since their inception, PIMs in Australia have received generally positive assessments.[323] There has also been positive judicial consideration on the benefit of PIMs. For example, in *R v Riscuta*, Burns J said:

> The role of the public interest monitor is an important one. Just as the courts have been traditionally regarded as the "guardians of the citizens right to privacy" … the [PIM] provides another layer of protection for private citizens who, unknown to those citizens, are sought to be made the subject of a surveillance warrant … [In the warrant issuing process, the PIM] is obliged to critically evaluate the material advanced in support of an application in order to determine whether to question the applicant police officer and/or make submissions on the hearing of the application. This will never be a perfunctory exercise; the public interest monitor must give real attention to the question whether the evidence and information offered by the party applying for the warrant is sufficient to satisfy the decision-maker of the existence of all applicable statutory preconditions and that the material is otherwise such as to justify such an intrusion into the privacy of the citizen in question.[324]

320 'Surveillance Devices Commissioner: Annual Data in Relation to the Administration of the Surveillance Devices Act 2007', *Department of Communities and Justice (NSW)* (Web Page, June 2025).

321 Public Interest Monitor (Qld), *Annual Report 2023-2024* (Report, 30 September 2024) 6; Qld PIM, *Submission 13*, 3.

322 Public Interest Monitor (Vic), *Annual Report 2023–24* (Report, 17 July 2024) 8–9 – of 270 'relevant applications' in 2023–24, the Victorian PIM appeared in 227. In addition to attendance at hearings, the PIM reviews draft application documents and discusses potential deficiencies with applicants: Victorian PIM, *Submission 24*, 2–6.

323 *Operation Prospect Report* vol 5, 762.

324 *R v Riscuta* (2017) 266 A Crim R 328, 337 [23].

8.14 In *Heery v Criminal Justice Commissioner Re Pierre Mark Le Grand*, White J said:

> In my experience [the PIM] has been of great assistance in balancing the competing interests of criminal investigations and the right to privacy.[325]

8.15 The 2020 Royal Commission into the Management of Police Informants in Victoria also commented on the importance of the type of oversight that PIMs provide in improving accountability and organisational performance.[326]

8.16 There was evidence to this review that state PIMs and the NSW SD Commissioner have continued to improve the quality of warrant applications and that their role is appreciated by issuing authorities. For example, the Inspector of the Law Enforcement Conduct Commission, Bruce McClintock SC, said that:

> There is no question that the Surveillance Devices Commissioner role has made a significant difference [in NSW] resulting in a real improvement to the quality of warrant applications put before Supreme Court Judges.[327]

8.17 Additionally, he observed that the quality of surveillance device warrant applications (which are subject to review by the NSW SD Commissioner) is often higher than that of telecommunications interception warrant applications (which are not subject to the NSW SD Commissioner's review). However, he also noted that there has been a positive improvement in all warrant applications since the establishment of the NSW SD Commissioner office. He also said that he had been 'told by several Supreme Court judges that they appreciate the role of the SD Commissioner in NSW.'[328]

Judges, independent oversight and a Royal Commission have praised the role of PIMs.

8.18 There was also evidence from state police forces that PIMs and the NSW SD Commissioner had improved efficiency and consistency in the warrant issuing system, including through the development of standardised templates and affidavits.

8.19 The New South Wales Police Force (NSW Police) confirmed that the input of the NSW SD Commissioner in the development of templates is 'overwhelmingly positive and, through the injection of fresh ideas and by challenging entrenched assumptions, resulted in a superior final product.'[329] It also said that these templates ensure any feedback from the NSW SD Commissioner and issuing authorities are 'implemented uniformly and without delay.'[330]

325 *Heery v Criminal Justice Commissioner Re Pierre Mark Le Grand* (2000) 110 A Crim R 465, 474 [33].
326 *Royal Commission into the Management of Police Informants* (Final Report, November 2020) vol 4, 185–6.
327 INSLM meeting with Bruce McClintock, 21 November 2024.
328 INSLM meeting with Bruce McClintock, 21 November 2024.
329 Letter from NSW Commissioner of Police to INSLM, 26 March 2025, 2.
330 Letter from NSW Commissioner of Police to INSLM, 26 March 2025, 1.

8.20 The NSW SD Commissioner described it as a 'key achievement' to work with NSW Police to develop and improve their template for an affidavit in support of a warrant application and has also issued detailed guidelines documents on the NSW SD Commissioner's involvement in the warrant application process and features of a quality affidavit.[331] The value of the NSW SD Commissioner was also recognised by Stephen Banks, Executive Member of New South Wales Council of Civil Liberties, who said:

> we're fortunate in New South Wales that the person who is appointed to that position is particularly knowledgeable and effective in achieving what has been achieved in New South Wales … in increasing the quality of submissions, applications for warrants by the various authorities, achieving uniformity in the applications so that they are easy to review by judicial officers whose role it is to issue the warrants.[332]

8.21 Victoria Police made a similar point, noting that the Victorian PIM has 'added value to the affidavit templates' and to the warrant issuing process more generally.[333] The Queensland Police Service said that the PIM process had created efficiencies in the warrant application process overall.[334]

New South Wales, Victorian and Queensland police say that the NSW SD Commissioner and PIMs have improved police templates, affidavits and guidelines.

Impact of state PIMs and NSW SD on warrant application timeliness

8.22 I was initially concerned that a Commonwealth PIM role may add delay to warrant applications, particularly urgent applications. I specifically discussed this with the Queensland Police Service, Victoria Police and NSW Police, as well as the PIMs and the NSW SD Commissioner. The vast majority of the evidence was the opposite: over time, PIMs have improved warrant processes and do not add any substantive delay to warrant applications, including urgent and time sensitive applications. Arrangements put in place in Victoria, New South Wales and Queensland have ensured that a PIM or the NSW SD Commissioner is available to consider urgent applications at short notice where required.

331 NSW SD Commissioner, *Submission 2*, 7.
332 Stephen Blanks, NSWCCL, *Public hearing transcript*, 20 February 2025, 9.
333 Letter from Acting Chief Commissioner, Victoria Police to INSLM, 24 February 2025.
334 INSLM meeting with Queensland Police Service, 18 December 2024.

8.23 The Queensland PIM said:

> It is my experience that the involvement of a PIM does not lead to difficulties in listing matters. While the Queensland PIM and Deputy PIMs are practising lawyers and have competing commitments, this does not generally cause issues with listing warrant applications, including urgent applications. A team of 3 (1 PIM and 2 Deputy PIMs) are available and this has been an appropriate number to adequately attend to the number of warrant applications made by Queensland law enforcement agencies. There is a good level of communication and cooperation between the applicant agencies' lawyers and the PIM/Deputy PIMs and amongst the PIM/Deputy PIMs.[335]

8.24 This assertion was supported by Queensland Police Service, which advised that it did not have any concerns about a PIM causing delay in warrant applications and had found the PIM to be as flexible as needed to enable the hearing of urgent applications on short notice.[336]

8.25 Victoria Police also advised that PIM review does not add unnecessary delays in seeking warrants and that it had not encountered any operational problems due to having a PIM in the process. It also noted that there are well-established administrative arrangements in place which ensure that PIMs are available at short notice, including for out-of-hours urgent applications.[337]

In Victoria and Queensland, police did not have any concerns about PIMs causing delay.

8.26 NSW Police said that:

> The [NSW SD Commissioner's] feedback assists by ensuring legal compliance, improving clarity, and reducing errors. Feedback from the [NSW SD Commissioner] may typically involve pointing out: specific legal requirements that have been overlooked or that have been insufficiently addressed; information that is vague, confusing or erroneous; and challenging the sufficiency of evidence. The [NSW SD Commissioner's] feedback helps [the NSW Police Force] present application to eligible Judges that are robust, legally comprehensive, and fit for purpose.[338]

8.27 However, it also said that the NSW SD Commissioner's 'involvement also comes with increased delays in warrant applications and opportunity cost to [police] through diversion of considerable time when similar functions are already performed [internally by NSW police].' NSW Police has an 'internal review process before seeking the [NSW SD Commissioner's] feedback supporting legal compliance, clarity and detection of errors' and that 'the addition of the [NSW SD Commissioner] draws resources away from [internal] oversight and quality control.'[339]

335 Qld PIM, *Submission 13*, 4.
336 INSLM meeting with Queensland Police Service, 18 December 2024.
337 Letter from Acting Chief Commissioner, Victoria Police to INSLM, 24 February 2025.
338 Letter from New South Wales Commissioner of Police to INSLM, 26 March 2025, 2.
339 Letter from New South Wales Commissioner of Police to INSLM, 26 March 2025, 2.

8.28 NSW Police acknowledged that the NSW SD Commissioner's input into the process had contributed to increased affidavit quality but considered that 'the net gain from [the Commissioner's] efforts is somewhat ambiguous.'[340] This can be contrasted with Victoria, where Victoria Police considered the PIM 'has added value to the affidavit templates and to the process more generally' and Queensland, where Queensland Police said the PIM process has created efficiencies in the warrant application process overall.[341]

8.29 The NSW SD Commissioner said that 'the AFP's concerns about the involvement of [PIMs] undermining investigations through delay is not borne out in the NSW experience.'[342] This was disputed to some extent by NSW Police, which said that '[t]he SDC's role has adversely impacted warrant timeliness' and noted that 'even short delays can result in loss of important evidence or increased risk to the public.'[343]

8.30 The NSW SD Commissioner provided evidence indicating that over the period July to September 2024 the Commissioner had been responsible for an average 'delay' of 1 hour and 4 minutes in urgent circumstances and a 'delay' of 2 hours and 20 minutes in non-urgent circumstances.[344] NSW Police said that these statistics do not include the time taken by NSW Police to respond if the NSW SD Commissioner makes submissions, which occurs in about 8% of cases. In relation to that 8% of cases, NSW Police advised that preparing a response 'typically takes a couple of hours and in rare instances, may take up to a day.'[345]

> Properly implemented and resourced, there is no reason to believe introducing a PIM would add delay.

8.31 I accept that NSW Police and the NSW SD Commissioner have different perspectives on delay. I am also mindful that New South Wales has only one NSW SD Commissioner and that they review close to 1,000 warrant applications per year. This is remarkable. It may be that, as the New South Wales Council for Civil Liberties said, 'fears of delay can be addressed by employing a full-time PIM with deputies who are properly resourced, allowing applications to be responded to in a timely manner.'[346]In contrast, Queensland and Victoria each have 3 part-time PIMs who deal with around 300 applications per year in those States. Furthermore, any 'delay' also needs to take account of the time saved by issuing authorities who have the benefit of the application process being improved by PIMs.

340 Letter from New South Wales Commissioner of Police to INSLM, 26 March 2025, 2.
341 Letter from Acting Chief Commissioner, Victoria Police to INSLM, 24 February 2025. INSLM meeting with Queensland Police Service, 18 December 2024.
342 NSW SD Commissioner, *Supplementary submission 25*, 3.
343 Letter from New South Wales Commissioner of Police to INSLM, 26 March 2025, 3.
344 NSW SD Commissioner, *Submission 2*, 13. Calculated on the basis of the sum of the period that a warrant application waited for the Commissioner's attention and when the Commissioner commenced dealing with the final product. This does not include time the Commissioner spent reviewing material that was found to be incomplete.
345 Letter from New South Wales Commissioner of Police to INSLM, 26 March 2025, 3.
346 NSWCCL, *Submission 10*, 6 [4.9].

Proposed nature of Commonwealth PIM

8.32 There were differing views about the role of and approach that should be taken by a Commonwealth PIM. The New South Wales Council for Civil Liberties considered that the role of a PIM should extend to oversight of AFP and ACIC compliance with *SLAID Act* warrants. [347] The joint academics considered that 'the role of the PIM should be more akin to a contradictor, tasked with representing the perceived interests of impacted parties.'[348] The Law Council of Australia said, 'the introduction of a public interest monitor regime could serve to promote an adversarial process in a manner similar to what occurs under the TIA Act for journalists.'[349]

8.33 In my view, the PIM role need not be seen as adversarial. Warrant applications are not court proceedings; they are closer to an inquisitorial process like a coronial matter. PIMs, like counsel assisting, are there to help test propositions and ensure that the decision-maker has as much relevant information as possible.

8.34 Of course, the Commonwealth PIM should be able to robustly raise matters that do not tend towards the issuing of a particular warrant or may oppose a warrant application where they consider it appropriate to do so.

> The PIM role need not be approached in an adversarial manner.

8.35 It should be the case that Commonwealth PIMs review all warrant applications, other than *emergency* authorisations and the very rare situation that an *urgent* application cannot wait for a PIM to be contacted.[350] Wherever possible, PIMs should provide constructive feedback on applications where required. It does not follow that PIMs will necessarily always feel the need to make submissions on a particular application.

8.36 Commonwealth PIMs having oversight of warrant outcomes would not be consistent with current Commonwealth government oversight arrangements for AFP and ACIC. However, as outlined below, a Commonwealth PIM could still perform a key role in incorporating the outcomes of oversight undertaken by IGIS and the Ombudsman into the warrant application process.

347 NSWCCL, *Submission 10*, 5.
348 Joint Academic Submission, *Submission 15*, 8.
349 Law Council, *Submission 23*, 58 [220].
350 As outlined above, experience in Victoria and Queensland is that PIMs are consistently available on short notice to deal with urgent applications: Letter from Acting Chief Commissioner, Victoria Police to INSLM, 24 February 2025; INSLM meeting with Queensland Police Service, 18 December 2024. In the case of urgent applications, PIMS should have authority to at least review a warrant application after it has been urgently issued and to raise any issues they identify. PIMs should also be heard at the time emergency authorisations that were issued internally are reviewed by an issuing authority.

Areas where the PIM would add value

8.37 Drawing on the experience of New South Wales, Queensland and Victoria as well as the experience of IPCO in the United Kingdom, there are a number of important ways that a Commonwealth PIM could improve the current system for the issuing of warrants. These include providing submissions on matters of public interest, ensuring feedback from oversight reviews is incorporated in submissions where relevant, providing feedback on templates and draft warrant applications and identifying cases where independent technical advice may be beneficial. Each of these is discussed in more detail below.

Providing submissions on matters of public interest

8.38 Matters of public interest should be considered as part of the issuing authority's decision whether to issue a *SLAID Act* warrant. The experience in New South Wales, Queensland and Victoria indicates that a Commonwealth PIM would add value to this consideration, including by drawing matters of particular relevance or risk to the issuing authority's attention and highlighting matters not addressed or not adequately addressed in warrant applications. This role would also potentially allow for streamlining of the current lengthy list of matters in the legislation that must be considered when determining whether to issue a *SLAID Act* warrant (discussed in Chapter 11).

8.39 The concept of 'public interest' is broad. It incorporates the public interest in preventing and investigating crime as well as the protection of privacy and other rights, transparency and accountability of government and protection of the rule of law.

8.40 It can be assumed that applications for warrants by police and criminal intelligence agencies will make the case for the public interest in preventing and investigating crime, and clearly this is an important consideration in assessing warrant applications.

8.41 In Queensland and Victoria, the existence of human rights legislation provides some guidance on the individual rights that are of interest to PIMs.[351] In the context of surveillance, privacy is clearly a key consideration – not only the privacy of the person or persons suspected of engaging in criminal activity (who must be regarded as innocent until proven guilty) but also the privacy of non-suspects. The impact on privacy is both an important consideration for the issuing authority (see Chapter 11) and an area where there is clear benefit in having input from an independent expert, not only the police or criminal intelligence agency perspective. Infringement of other rights including property rights may also be relevant, especially for DDWs.

351 *Human Rights Act 2019* (Qld); *Charter of Human Rights and Responsibilities Act 2006* (Vic). At a Commonwealth level there is no equivalent; however, regard should be had to Australia's international obligations, including under the *International Covenant on Civil and Political Rights* and particularly art 17 in relation to privacy: *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) art 17.

8.42 Another area where PIMs can potentially make valuable submissions is in the protection and preservation of legal professional privilege (LPP) in the public interest.[352] It is noted that the NSW SD Commissioner said that his role 'routinely' involves providing submissions to issuing authorities on the types of conditions that might be imposed on a warrant to protect privilege and that conditions concerning privilege are regularly imposed.[353] Similar comments were made by the Queensland PIM, who noted that almost all warrants have a condition that protects and preserves LPP.[354]

8.43 Input from a Commonwealth PIM could go to both the risk of privilege being infringed by collection and the adequacy of procedures to be implemented to protect privilege. These submissions need not always be directed to preventing collection but may, for example, go to the need for conditions to prevent improper disclosure of privileged information.

8.44 Similarly, it could be expected that a PIM would make submissions about the public interest in a free press and the protection of journalist's sources.

8.45 The Media Entertainment and Arts Alliance and the Alliance for Journalists' Freedom submitted that, because of the public interest in a free press, there should be special arrangements for media organisations or journalists to be notified and then have an opportunity to make submissions before a warrant is executed in relation to them.[355] There is currently a limited role for submissions from a 'public interest advocate' in relation to applications for journalist information warrants under the TIA Act.[356] Recent reviews have identified the need for submissions from this type of office to address the public interest in preserving the confidentiality of journalist sources and in assisting to exchange information between journalists and members of the public to facilitate reporting of matters in the public interest in the wider law enforcement context.[357] This has been accepted by the government.[358] As explained in Chapter 11, the current criteria for considering the public interest in journalism before issuing a *SLAID Act* warrant are narrow and unlikely to address most situations where journalistic information may be identified.

---

352 The NSW SD Commissioner observed that 'in circumstances where privilege is at risk of being compromised by surveillance device use, the NSW Surveillance Devices Commissioner routinely highlights this to the eligible Judge in submissions' and '[s]trategies have been settled to manage the risk of compromising privilege.' In this regard, the Commissioner observed that they provide guidance 'as to specific conditions that can be applied' to protect legal professional privilege and that 'such additional conditions are regularly imposed': NSW SD Commissioner, *Submission 2*, 16.

353 NSW SD Commissioner, *Submission 2*, 16.

354 INSLM meeting with David Adsett, Qld PIM, 11 September 2024.

355 MEAA, *Submission 19*, 2–3; AJF, *Submission 7*, 5 [4.2]–[4.5].

356 *TIA Act* s 180X.

357 PJCIS, *Inquiry into the Impact of the Exercise of Law Enforcement and Intelligence Powers on the Freedom of the Press* (Report, 26 August 2020) Recommendation 2.

358 The government has agreed to expand the Public Interest Advocate regime to all warrants, including *SLAID Act* warrants that relate to journalists or media organisations, where the warrants are related to investigations involving the unauthorised disclosure of government information or a secrecy offence: Australian Government, *Australian Government Response to the Parliamentary Joint Committee on Intelligence and Security report: Inquiry into the Impact of the Exercise of Law Enforcement and Intelligence Powers on the Freedom of the Press* (Government Response, October 2020) 3 (Recommendation 2).

8.46 It may be necessary for PIMs to work with media organisations over time to understand the arguments they would put in this regard in a general sense so that PIMs are able to make appropriate submissions on specific cases if the need arises. This would avoid the need for a specific regime for any applications that relate to journalists or media organisations as originally proposed by the PJCIS.[359] It would also ensure that submissions on the public interest in protecting journalists' sources and a free press are not narrowly confined to cases involving secrecy offences and direct surveillance of journalists or media organizations.

8.47 This list of matters of public interest is not intended to be exhaustive. What, if any, submissions may be appropriate will vary depending in the case. The point is that there are many areas where an issuing authority could benefit from independent submission on public interest matters to assist them in assessing warrant applications. The existence of a PIM who makes such submissions should also provide greater public confidence that matters such as human rights and protection of specific categories of information are consistently raised and rigorously tested.

PIMs may support compliance with international human rights obligations

8.48 There are several areas where the introduction of a Commonwealth PIM may support compliance with Australia's international human rights obligations (discussed in Chapter 17) including by identifying and suggesting measures to mitigate the risk of possible non-compliance with such obligations associated with the exercise of *SLAID Act* powers.

8.49 Where operations are conducted jointly with foreign agencies, depending on the facts, a Commonwealth PIM may make submissions on the risk of information being shared that could be contrary to Australia's position on the death penalty. Similarly, there could be cases where there was a risk of Australian information making its way to a third party where there is a risk of torture or other human rights abuses. The existence of a Commonwealth PIM who can make submissions in this regard may go some way toward addressing concerns the PJCHR has consistently raised about such risks.[360]

8.50 The European Court of Human Rights has observed that, because there are limited avenues to challenge or seek review of covert warrants, 'it is essential that the procedures established should themselves provide adequate and equivalent

359 *PJCIS SLAID Report* Recommendation 19. This approach is consistent with the PJCIS' recommended approach in PJCIS *Inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press* (Report, 26 August 2020) Recommendation 2.

360 See, for example, PJCHR, *Human Rights Scrutiny Report* (Report No 1 of 2021, 3 February 2021) 33 [1.75]–[1.76]; PJCHR, *Human Rights Scrutiny Report* (Report No 3 of 2021, 17 March 2021) 94 [2.90]–[2.91], 98 [2.103(f)].

guarantees safeguarding … rights.'[361] In that context, the PJCHR and Australian Human Rights Commission concluded that PIMs are a 'valuable safeguard to protect the interests of the affected person in any warrant application or review proceedings.'[362] The Australian Human Rights Commission observed:

> A PIM would act as a counterbalance to ensure that these measures are used proportionately and only when strictly necessary. The PIM's role would include providing independent oversight to ensure that the issuing authority critically evaluates the necessity and proportionality of each warrant application, ensuring that the interests of those affected by the warrants are represented and considered, and ensuring that the use of these intrusive powers complies with human rights standards. An additional advantage of the PIM would be strengthening public confidence in the warrant process by increasing transparency and accountability without compromising operational security. [363]

8.51 As noted by the Queensland PIM, the 'existence of the PIM may act as a moderating influence on the ambit of warrant applications, encouraging a more proportionate response by law enforcement.'[364]

8.52 Most civil society submissions to this review gave similar reasons for supporting the introduction of a Commonwealth PIM, although some preferred the IPCO model of a single agency responsible for oversight and issuing warrants.[365]

There are many public interest issues that would benefit from PIM submissions, including privacy, LPP, the role of a free press and preventing inappropriate sharing of data with third parties.

361 *Roman Zakharov v Russia* (European Court of Human Rights, Grand Chamber, Application No 47143/06, 4 December 2015) [233].

362 AHRC, *Submission 21*, 9 [29] 9 citing PJCHR, *Human Rights Scrutiny Report* (Report No 3 of 2021, 17 March 2021) 94 [2.91], 98 [2.103(f)].

363 AHRC, *Submission 21*, 10 [31].

364 Qld PIM, *Submission 13*, 4.

365 HRLC, *Submission 5*, 8 (Recommendation 1); QCCL, *Submission 6*, 7; AJF, *Submission 7*, 4 [3.2]; NSWCCL, *Submission 10*, 5–6; Joint Academic Submission, *Submission 15*, 9 (Recommendation 3(b)); IAA, *Submission 16*, 2; AHRC, *Submission 21* (Recommendation 5); Law Council, *Submission 23* (Recommendations 37–39). Others opposed PIMs on the basis that realising a dedicated warrant issuing body similar to IPCO by establishing an investigatory division or list in the ART would be a better solution: Marcus Smith, *Submission 1*, 2; Philip Glover, *Submission 8*, 5.

Identifying cases where independent technical advice may be required

8.53 As outlined in Chapter 9, in the context of highly technical warrants such as *SLAID Act* warrants, it is essential that an issuing authority has access independent technical advice.

8.54 However, having *access* to independent technical advice is not the same as always knowing when that advice may be beneficial. PIMs could potentially assist issuing authorities in this regard. Simply by being an independent set of eyes that can scrutinise warrant applications, PIMs increase the likelihood that relevant technical questions will be raised. However, the proposed role of PIMs includes a number of features that suggest they will be of particular assistance to issuing authorities in this regard. First, through regular interactions with oversight bodies, PIMs will be able to discuss emerging technologies with those independent bodies. Second, it is anticipated that PIMs will participate in all of the periodic briefings provided by the new technology advisory panel (see Chapter 9). PIMs should also have direct access to the technical advisors in the same way that in-house counsel from IPCO do and, in this way, can ask questions on novel applications at the draft warrant stage to help to determine whether the matter is one on which independent technical input may be beneficial.

> PIMs increase the likelihood that relevant technical questions will be raised.

8.55 As there will likely be fewer PIMs than issuing authorities and PIMs will regularly interact with each other and their state counterparts, including on technical issues, the level of technical skills in the group of PIMs can be expected to increase over time. The NSW SD Commissioner said that the PIM can 'become a repository of technical expertise, or a conduit to other sources of expertise, and can facilitate access for issuing authorities as needed.'[366]

Feedback on draft warrant applications

8.56 As outlined above, the experience in New South Wales, Victoria and Queensland has been that the introduction of state PIMs and a NSW SD Commissioner has led to an increase in the efficiency of the warrant system. This has been primarily through feedback on draft warrants and improvements to templates and guidance on information that should be provided.

8.57 The Queensland PIM highlighted the constructive approach that applicant agencies have taken to addressing deficiencies in warrant applications highlighted by the PIM:

366 NSW SD Commissioner, *Submission 2*, 11. The Victorian PIM said that any independent technical advice should be disclosed to the PIM and warrant applicant before the application is decided: Victorian PIM, *Submission 24*, 8.

> Relatively few applications are opposed. Applications are often the subject of preapplication discussion and negotiation between the PIM and the lawyer representing the applicant agency. This will often result in modification of the draft warrant or the application material, e.g. additional information in the applicant's affidavit.[367]

8.58 In the UK where warrant approval and oversight and review functions are part of the same independent agency, IPCO's in-house lawyers can be provided with applications in draft and may, along with the inspectors, provide non-binding guidance, in advance of an application being submitted to a judicial commissioner. Review by in-house lawyers at IPCO is generally confined to new, novel or contentious matters. The in-house lawyers also provide real-time advice to judicial commissioners on pending applications.[368]

8.59 Although I acknowledge that internal AFP and ACIC mechanisms can play a role in providing feedback on templates and draft warrant applications, the benefit of independent feedback on templates and draft warrant applications should not be underrated. This type of feedback assists in ensuring issuing authorities are receiving the best possible applications and that, as far as possible, errors and omissions are rectified before the matter goes to the issuing authority. It can also enhance public confidence in the system in a way that internal review by the applicant agency cannot.

> The benefit of independent feedback on templates and draft warrant applications should not be underrated.

8.60 As there will likely be fewer PIMs than issuing authorities, the PIMs will have the benefit of seeing a larger number of applications and applications from different agencies. This, combined with their ability to spend time becoming familiar with oversight outcomes and reports and discuss relevant matters with other PIMs, will put PIMs in a strong position to spot inconsistencies with earlier applications or reports. They can then draw these to the attention of agencies at an early stage and, if not resolved, make submissions to the issuing authority on the point.

8.61 IPCO has also issued formal guidance to warrant applicants setting out the approach IPCO will take to authorisation (including what is expected in warrant applications). The fact that it has been able to do this in a public document is to be commended. Although these guidelines are non-binding, it is intended that they help judicial commissioners achieve greater consistency in approach.[369] A similar approach in Australia would be beneficial both to public transparency and to agencies in preparing warrant applications. Such guidance could be issued by the senior judge identified as head of the panel of retired judges appointed as issuing authorities (Chapter 7).

367 Qld PIM, *Submission 13*, 4.
368 Email from IPCO to INSLM, 25 July 2025.
369 IPCO, *Advisory Notice 1/2018: Approval of Warrants, Authorisations and Notices by Judicial Commissioners* (Document, 8 March 2018) 1 [1]; see also *Investigatory Powers Act 2016* (UK) s 232(2).

Feedback on outcome of oversight processes

8.62 One of the functions of the Commonwealth PIMs should be incorporating relevant oversight findings into feedback on applications and, where necessary, submissions to the issuing authority.

Benefits of feedback being incorporated into the warrant issuing process

8.63 Once a warrant has been issued and executed, IGIS and the Ombudsman can review the warrant to determine whether that execution was consistent with what the issuing authority approved. Among other things, they may identify any systemic issues that may affect many warrants. The oversight process is discussed further in Chapter 16. For present purposes, the key point is that the oversight processes can produce information that would be relevant for a future issuing authority to know.

> Issuing authorities could benefit from feedback from the work of oversight bodies.

8.64 Examples of things identified by oversight bodies that might provide an issuing authority with a more complete and accurate picture of a warrant application include agency systems not actually being set up to delete material as required,[370] failure to revoke warrants as required,[371] lack of candour in applications,[372] collection systems recording information that was unexpected and/or unauthorised,[373] whether conditions were complied with, and how privacy was actually affected (including through international sharing of information). Reports that indicate thorough inspections have *not* identified any legality or propriety issues are also relevant. These and similar points can go to risk and proportionality and also to whether the issuing authority should place conditions on a warrant.

8.65 Agencies will not necessarily agree with oversight findings. This does not make them irrelevant. Experienced issuing authorities are well equipped to deal with conflicting views.

8.66 In the United Kingdom, inspection, approval and authorising functions sit within the same body: IPCO. The work of the inspectors feeds into the considerations of the judicial commissioners and those authorising data requests. IPCO's in-house lawyers review applications where judicial commissioners provide comments and

370 IPCO has underlined in recent years persistent issues with IT systems used by law enforcement agencies that make it practically difficult to delete intercept material at the end of operations. It recommended urgent changes to update these IT systems: Investigatory Powers Commissioner (UK), *Annual Report of the Investigatory Powers Commissioner 2022* (Report, 24 November 2023) 9, 68 [13.40]–[13.42].

371 Ombudsman, *Report to the Attorney-General on Agencies' Compliance with the Surveillance Devices Act 2004 (Cth) for Commonwealth Ombudsman Inspections Conducted from 1 January to 30 June 2024* (Report, September 2024) 22 (AFP), 25 (ACIC).

372 Issues have arisen in New Zealand, Canada, United States and the United Kingdom. See Chapter 9 and Annex B.

373 See, for example, IGIS, *Annual Report 2022–23* (Report, 25 September 2023) 100.

feedback to ensure that this information is communicated to inspectors who can then incorporate it in future inspections and reviews.[374]

8.67 There are mechanisms in Queensland and New South Wales for issuing authorities to receive reports prepared by state police on individual surveillance device warrants that they issued. I understand that in practice, these reports also go to the PIM or NSW SD Commissioner, who can incorporate them into future submissions as required.[375]

8.68 The NSW SD Commissioner said they have access to information that allows them to be 'in a position to feed information about actual application of authority back into the authorisation process, to enhance that process.'[376]

There are models in other jurisdictions where a feedback loop with oversight is a valuable part of the warrant issuing process

8.69 AGD accepted that sharing of information on the outcomes of inspections and inquiries 'may also assist issuing authorities to understand how powers are used in practice, and potential risks in the execution of those powers.'[377] However, the department cautioned that practical implementation of a feedback loop between relevant oversight agencies and the issuing authority would carry complexity because of 'the number and geographic distribution of issuing authorities' and 'how to ensure such information is delivered in a manner that is relevant to issuing authorities.' I agree and consider that PIMs are the most effective way to synthesise and deliver this information.

8.70 The Ombudsman indicated they supported the establishment of a feedback loop to allow issuing authorities to gain greater understanding of how powers are being used, noting that this may have particular benefit for novel and technically complex warrant powers like *SLAID Act* powers.[378] IGIS considered that establishing a feedback loop with issuing authorities is a matter for government. However, IGIS observed that such a feedback loop must be implemented with appropriate

374 Email from IPCO to INSLM, 25 July 2025.

375 In Queensland, there is a requirement to make a report to the judge or magistrate who issued the warrant or to the PIM as stated in the warrant: *Police Powers and Responsibilities Act 2000* (Qld) s 357(2). Issuing authorities ordinarily direct that reports are given only to PIMs: Public Interest Monitor (Qld), *Annual Report 2023-2024* (Report, 30 September 2024) 8. In New South Wales, reports about use must be furnished to the judge or magistrate who issued the warrant and the Attorney General (NSW): *Surveillance Devices Act (No 64) 2007* (NSW) s 44. In practice, reports are provided to the NSW SD Commissioner as the Attorney General's delegate: NSW SD Commissioner, *Submission 2*, 19. The NSW SD Commissioner said that his office reviews all use reports 'closely and sought clarification in appropriate circumstances'; however, he considers that there should be strengthened statutory mechanisms for his office to ask agencies for clarification regarding use reports: NSW SD Commissioner, *Submission 2*, 19.

376 NSW SD Commissioner, *Submission 2*, 14.

377 AGD, *Submission 20*, 13.

378 Ombudsman, *Submission 11*, 6–7.

legislatives and administrative mechanisms – in particular, there would need to be clear authority to disclose information.[379]

8.71 The Human Rights Law Centre, New South Wales Council for Civil Liberties, Law Council of Australia and Internet Association of Australia underlined the importance of strengthening mechanisms for information sharing that gives issuing authorities and PIMs visibility over how warrants are executed and provide oversight outcomes that can improve the scrutiny applied in issuing warrants.[380] Stephen Blanks, on behalf of the New South Wales Council for Civil Liberties, underlined that it is 'important to ensure that the various different aspects of that regulatory system can liaise with each other and exchange information and gain insights from each other's activities.'[381] Tim Game SC, on behalf of the Law Council of Australia, emphasised the importance of a PIM-like office in highlighting relevant issues contained in oversight outcomes to the issuing authority.[382]

Role of the PIM in a feedback loop

8.72 It is not practical to ask all issuing authorities to read all IGIS and Ombudsman reports in case they contain something that may be relevant to a future warrant application. Furthermore, particularly for IGIS, very little detail is publicly reported. Asking the oversight bodies themselves to make submissions is also impractical unless an IPCO model, where oversight and issuing functions form part of the same body, is adopted. Asking police and criminal intelligence agencies to include reference to what they may consider to be relevant oversight findings in their applications undermines the purpose of independence in oversight and risks relevant information being excluded. The remaining option is to incorporate this role into the work of the Commonwealth PIMs.

> Incorporating relevant oversight findings into feedback on applications and where necessary submissions should be a function of the Commonwealth PIMs.

8.73 This means it would be a function of Commonwealth PIMs to be across relevant oversight findings and reports and to be able to synthesise that information into feedback on warrant applications and, where necessary, submissions to issuing authorities. To facilitate this, it is necessary to ensure that statutory secrecy provisions do not prevent PIMs from accessing relevant reports and findings.[383] Normal Commonwealth security policy and procedures should apply to ensure appropriate protection of information and the secrecy offences in pt 5.6 of the *Criminal Code* would also apply to any improper disclosure by a PIM or an issuing authority.

379 IGIS and INSLM, *Agreed Record of Meeting* (28 February 2025) 1.
380 HRLC, *Submission 5*, 8 (Recommendation 2); Law Council, *Submission 23*, 69 [266]; IAA, *Submission 16*, 2.
381 Stephen Blanks, NSWCCL, *Public hearing transcript*, 20 February 2025, 11.
382 Tim Game, Law Council, *Public hearing transcript*, 19 February 2025, 48.
383 IGIS and INSLM, *Agreed Record of Meeting* (28 February 2025) 1.

8.74 The other side of the feedback loop is providing feedback to oversight bodies on warrants where issuing authorities have particular concerns or have added conditions for a particular purpose. Commonwealth PIMs could also play a role in providing that feedback to oversight bodies. Those independent oversight bodies could then take that into account in planning and conducting future inspections.[384]

8.75 Closely linked to understanding oversight findings is an understanding of relevant agency policies, including those that may have changed since an oversight report. Understanding of the adequacy of agency policies will also be needed if simplified issuing criteria are implemented (see Chapter 11 and Recommendation 12(e)).

Recommendation 7: There should be Public Interest Monitors whose role includes providing submissions on matters of public interest and feedback from oversight processes, identifying matters where independent technical advice may be required and providing comments on draft warrant applications and templates.

Selecting and resourcing Commonwealth PIMs

8.76 As with the appointment of issuing authorities, it would be beneficial for Commonwealth PIMs to be appointed through a transparent, merit-based selection process. The selection criteria should be based on the expected scope of the role. The mix of skills and qualifications of the state PIMs and NSW SD Commissioner may provide some useful guidance. For example, as noted by the Victorian PIM:

> PIMs must also be skilled at interpreting legislation and conversant with current legislation and case law relevant to the issues they must address in carrying out their statutory functions and powers. An awareness and understanding of law enforcement methods and practices together with knowledge of current technology and the way in which it can be used is also essential as is a broad awareness of the methods and practices of those who may seek to act in breach of the criminal law.[385]

8.77 Where warrant applications raise novel questions or require complex judgements of fact and law, the presence of a PIM with substantial legal experience would probably be of particular benefit to issuing authorities. As the Law Council of Australia has noted DDWs are likely to raise complex questions as well as a risk of

384 To be clear, it would remain a matter for the independent oversight bodies to decide what, if any, action to take in response to such feedback. It is not proposed that PIMs should in any way be able to direct the work of independent oversight bodies, only that PIMs can provide relevant information about concerns to oversight bodies which they can then take into account.

385 PIM – Victoria, *Submission 24*, 1.

consequences for third parties.[386] The same could be said for NAWs given their breadth and, depending on how they are executed, some ATWs.

8.78 Commonwealth PIMs should also be expected to work with PIMs from other jurisdictions and the NSW SD Commissioner as well as human rights groups, legal groups and media groups to understand and be able to advocate on a range of public interest issues. This was recognised by the Media, Entertainment and Arts Alliance, which said that:

> [in respect of the] purposes, tools and training, systematic engagement and reporting – the design of the office ought to be intended to put the PIM in a position which is as close to that of a journalist or media organisation would be ...[387]

8.79 There would also be benefit in Commonwealth PIMs having clear independence – for example, by being appointed as statutory officers of some type. Their terms of appointment should include limited and clearly defined grounds of removal.[388]

8.80 The PIMs and NSW SD Commissioner each operate on different models, but all are small:

- Victoria has a PIM and 2 deputies. Each is employed by the state on a parttime basis.[389] The current Principal PIM is a former Deputy President of the AAT.
- Queensland has a PIM and 2 deputies. All are barristers in private practice who undertake PIM work as required. The Queensland PIM operates on a cost recovery model – police are charged a prescribed fee to cover the cost of the PIM's time.[390]
- The NSW SD Commissioner is one person employed full-time in the NSW Public Service[391]and assisted by a 'project officer.'

8.81 The number of Commonwealth PIMs, their distribution nationally and the process for recruiting and employing them are all matters of administration to be worked through by the department as part of ensuring the integrity and robust oversight of warrant issuing processes. As with issuing authorities, the allocation of a 'principal' PIM to provide leadership and guidance would be a sound approach.[392]

386 Law Council, *Submission 23*, 36 [127]; Law Council, Submission No 21 to PJCIS, *Review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (9 March 2021) 55 [114]–[116].

387 MEAA, *Submission 19*, 4. Note that MEAA's preferred option was for media organisations themselves to be heard on warrant applications.

388 Law Council, *Submission 23*, 59 [226].

389 The Principal PIM and deputy PIMs are appointed by the Governor in Council: *Public Interest Monitor Act 2011* (Vic) ss 6–7; there are currently 2 deputy PIMs: Victorian PIM, *Submission 24*, 1.

390 Remuneration is on a fee for service basis at a fixed hourly rate. The PIM and deputy PIMs are appointed by the Governor in Council: *Crime and Corruption Act 2001* (Qld) s 324; *Police Powers and Responsibilities Act 2000* (Qld) s 740; Qld PIM, *Submission 13*, 2.

391 *Surveillance Devices Act (No 64) 2007* (NSW) s 51A.

392 This is the practice in both Victoria and Queensland, where, in addition to the Principal PIM, one or more deputy PIMs may be appointed: *Public Interest Monitor Act 2011* (Vic) ss 6–7; *Police Powers and Responsibilities Act 2000* (Qld) s 740.

8.82 The main variable will be how many warrants are to be covered by the new system. Recommendations in this review are necessarily limited to *SLAID Act* warrants. As noted earlier, many of the concerns with the system for issuing complex, covert and invasive warrants that are not readily subject to review by the courts extend well beyond the *SLAID Act*. This is a matter that could be considered by the current Home Affairs ESR project.

Interaction with state PIMs and SD Commissioner

8.83 Because this report has made multiple refences to state PIMs and the NSW SD Commissioner, it is worth pointing out that the jurisdiction of those bodies does not extend to any AFP or ACIC warrants and thus does not apply to *SLAID Act* warrants.

8.84 State PIMs and the NSW SD Commissioner are, appropriately, focused on warrants used by state agencies. This can include warrants under Commonwealth legislation, particularly the *TIA Act*.

8.85 If the PIMs proposed by this review are to be extended to all covert Commonwealth warrants then, depending on the outcomes of the ESR project, this will require some negotiation with states. For example, in Queensland and Victoria, where state PIMs already have a role in making submission on *TIA Act* warrants used by state authorities, it would seem likely that such a role would be retained. In states that do not have a PIM equivalent role for Commonwealth warrants (which currently includes New South Wales), the introduction of this type of role could be encouraged. If it is not, the Commonwealth PIM could fill the void. These points are only observations – the role of state PIMs is beyond the scope of this review.

Chapter 9: Other improvements to the warrant issuing system

9.1 Changes to the warrant issuing system to use retired judges and introduce Commonwealth PIMs are both critical, but they are not the only changes needed to make the warrant issuing system fit for purpose. This chapter discusses other key changes that are needed: access to independent technical advisors; a clearer (and higher) duty of candour; and, an effective secretariat to amongst other things ensure warrant applications are independently allocated.

Independent technical advisers are essential

9.2 Technical complexity is increasingly a feature of a range of modern warrants. As AFP said:

> telecommunications interception, surveillance device and computer access warrants are often very technical in terms of the particular method of access to be carried out under the warrant.[393]

9.3 Many *SLAID Act* warrants involve the use of particularly sophisticated techniques. For example, AFP gave evidence that DDWs may involve disparate technical considerations '… where the specific method of disruption may be different on a case-by-case basis depending on the size of a target computer and the software and hardware used by [a] suspect.'[394] ACIC noted that for NAWs, 'significant time is required once a warrant is issued to identify, assess, develop and test the technical options available prior to operational activity occurring.' Additionally, because of the sophisticated nature of technologies that NAWs target, there is a need to develop 'bespoke and necessarily complex targeting methodologies.'[395] ACIC identified technical complexity and the need to develop new capabilities as one of the reasons they had not yet used any DDWs or ATWs.[396]

9.4 At the time *SLAID Act* warrants were introduced, the primary reason for the need for new powers was that criminal groups are using sophisticated technology, including encryption and anonymising technology.[397] There is no evidence that the technology is becoming simpler. To the contrary: there is evidence that new technologies such as artificial intelligence are making the environment *more* complex.[398]

393 AFP, *Submission 18*, 9 [50].
394 AFP, *Submission 18*, 9 [51].
395 ACIC, *Submission 17*, 8.
396 ACIC, *Submission 17*, 3, 5.
397 Revised Explanatory Memorandum [2]–[3]; Commonwealth, *Parliamentary Debates*, House of Representatives, 3 December 2020, 10431 (Peter Dutton MP, Minister for Home Affairs).
398 ASD, *ASD Cyber Threat Report 2023–24* (Report, 20 November 2024) 1. For more information on technological change leading to a 'dramatic shift in the complexity, scale and tempo of some security challenges', including because of artificial intelligence, quantum computing and generative AI, see Department of the Prime Minister and Cabinet (Cth), *2024 Independent Intelligence Review* (Report, 21 March 2025) 25–6 [4.23]–[4.25] (*2024 Independent Intelligence Review*).

Understanding the technology to assess proportionality

9.5 To assess the proportionality of the effect of a warrant, the decision-maker needs to understand the technology enough to independently weigh the likely impact and risks – not only on the person or persons who are the target of the warrant but also on other people and on infrastructure (for example, the risk of introducing potential systemic vulnerabilities).[399]

> The issuing authority needs to understand the technology enough to ask the right questions in order to properly assess risk, impact and proportionality.

9.6 To some extent, the decision-maker should rely on submissions made by the applicant. AFP and ACIC said that they make specialists available to answer any questions an issuing authority may have. At the public hearing an AFP witness said that they were also aware of occasions where slides had been used to try to 'better articulate and understand what can be quite complex concepts.'[400]

9.7 However, I was concerned that both AFP and ACIC seemed to suggest that it was not necessary for the issuing authority to have a strong grasp of the technology that they were authorising for use. AFP said that the 'technical nature of the capability is only relevant to the extent that it directly relates to [the] legal thresholds' and that it is not necessary to 'specify the exact technical capability to be used, which enables AFP to adjust and tailor its approach across the course of the warrant execution.'[401] Similarly, ACIC said that it may utilise bespoke approaches and the technology may change through the life of the warrant.[402]

9.8 It may be necessary and proportionate to authorise a range of capabilities under a warrant, but to me this increases, rather than decreases, the need for the issuing authority to understand the full spectrum of what they are authorising.

9.9 It is important that AFP and ACIC continue to make technical experts available and to explain the technology they propose to use. However, reliance on advice from the

399 On risk to infrastructure, see Australian Information Industry Association (AIIA), *Submission 12*, 2; IAA, *Submission 16*, 2–3.

400 Rob Nelson, Commander, AFP, *Public hearing transcript*, 20 February 2025, 28 [15]–[20]. See also ACIC, *Submission 17*, 9; AFP, *Supplementary response 29,* 2.

401 AFP, *Submission 18*, 9 [51]–[52].

402 ACIC, *Submission 17*, 9.

agency being overseen was noted as diminishing actual or perceived independence over time in the context of oversight.[403] The same must be said for issuing warrants.

9.10 It enhances independence and rigour in decision-making to have access to independent technical advice as part of the warrant issuing process. In practice, such advice can help decision-makers know what questions to ask.

> Independence and rigor in decision-making are enhanced by having access to independent technical advice.

General agreement that access to independent technical advice is needed

9.11 The need for independent technical advice in the context of assisting oversight agencies has been highlighted in successive reviews.[404] Most recently, the 2024 Independent Intelligence Review found that the 'increasing complexity of the technological landscape' complicates the task of oversight agencies 'to understand the nature and operations of agencies' capabilities and the technological context in which agencies operate.'[405]

9.12 Submissions from civil society and the Australian Human Rights Commission expressed strong support for establishing an independent technical advisory panel to assist the issuing authority.[406] The Australian Information Industry Association said '[t]he complex and highly technical nature of the warrants introduced by the *SLAID Act* requires decision-makers to have access to expertise that ensures actions are both operationally feasible and proportionate.'[407] The Australian Human Rights Commission raised a similar concern, adding that 'complexity is only likely to increase as technologies continue to develop.'[408] The Law Council of Australia said that the ability to seek independent technical advice is 'necessary to preserve the appearance of independence in the issuing process.'[409]

9.13 AGD accepted that 'independent advice may assist issuing authorities to understand, interrogate and determine warrant applications.'[410] In my view, it is a significant deficiency in the current system for issuing warrants that issuing authorities do not have access to independent technical advice.

403 *2024 Independent Intelligence Review* 116–17 [18.41]–[18.42].
404 *2019 Comprehensive Review* vol 3, 281, Recommendation 173.
405 *2024 Independent Intelligence Review* 116–17 [18.41].
406 Law Council, *Submission 23*, 60–2 (Recommendations 40 and 41); AHRC, *Submission 21*, 10–11 (Recommendation 6); Joint Academic Submission, *Submission 15*, 8–9. See generally, regarding the need to strengthen mechanisms for independent technical advice, QCCL, *Submission 6*, 6–7; MEAA, *Submission 19*, 2–3.
407 AIIA, *Submission 12*, 2.
408 AHRC, *Submission 21*, 10 [32].
409 Law Council, *Submission 23*, 60 [228].
410 AGD, *Supplementary Submission 28*, 5.

It is a significant deficiency in the current system for issuing warrants that issuing authorities do not have access to independent technical advice.

United Kingdom Technical Advisory Panel model

9.14 In the United Kingdom, the role of the independent Technology Advisory Panel (TAP) in supporting the Investigatory Powers Commissioner and judicial commissioners is now well established. The statutory function of the TAP is to provide advice to the Investigatory Powers Commissioner, the Secretary of State and ministers about:

- the impact of changing technology on the exercise of investigatory powers.
- the availability and development of techniques to use such powers while minimising interference with privacy.[411]

9.15 The TAP is highly valued in the UK, including for its role in advising judicial commissioners. The Investigatory Powers Commissioner, Sir Brian Leveson, said:

> The Technology Advisory Panel—comprising distinguished academics and experts in computer science and mathematics—plays a crucial role at IPCO by advising me, the Judicial Commissioners, and Inspectors on the use of technology in relation to investigatory powers. I particularly value their ability to interrogate complex technical issues, highlight those most pertinent to my oversight responsibilities and present their findings in a way that enables us to fully consider the legal implications.[412]

9.16 The Investigatory Powers Commissioner appoints TAP members under the *Investigatory Powers Act 2016* (UK).[413] The TAP was originally made up of 3 and now 6 highly qualified members, each appointed on a part-time basis.[414] The current Chair of the TAP, Professor Dame Muffy Calder, is a distinguished computer scientist with expertise in computational modelling and is former Chief Scientific Advisor for Scotland. Other members of the panel are distinguished academic mathematicians with experience in undertaking advisory roles across government. Others have practical experience in the cryptography and cybersecurity field in government, law enforcement and industry roles.[415] Members of the panel are

411 *Investigatory Powers Act 2016* (UK) s 246(1)(a), (b).
412 Email from IPCO to INSLM, 25 July 2025
413 *Investigatory Powers Act 2016* (UK) s 247(1).
414 Investigatory Powers Commissioner (UK), *Annual Report of the Investigatory Powers Commissioner 2023* (Report, 20 December 2024) 22 [5.3].
415 The biographies of the current members of the Technology Advisory Panel are publicly available on the IPCO's website: 'Who We Are: Technology Advisory Panel', *IPCO* (Web Page).

remunerated on an agreed daily rate. In 2023–24, each member of the panel contributed an average of 21 days to TAP duties.[416]

9.17 As a matter of practice, the TAP's key priorities have been defined by agreement with the Investigatory Powers Commissioner to include advising issuing authorities on individual warrant applications and proactive guidance:

> Given that a key role overarching all the Commissioner's work is to ensure that powers are used in such a way as to minimise interference with privacy, advice may be sought from the TAP on any scientific or technological aspect of methods being used in the exercise of investigatory powers, either in a specific case or in a more general context.[417]

9.18 Examples of the types of proactive guidance provided by TAP include an aide-memoire for proportionality considerations relevant to assessing privacy intrusiveness and recent work on an AI Proportionality Assessment Framework.[418] While the TAP no doubt provides more detailed guidance at a classified level, the fact that frameworks for assessment are published is a boost to the transparency of how decisions are made. I consider that there would be significant benefit from similar public guidance documents being issued in the Australian context, subject to the usual requirements of operational security (which also apply in the United Kingdom).

9.19 TAP advice is not required on every warrant, but their dual role of providing general briefings to decision-makers on new technologies and, where needed, specific advice on novel applications is valuable. IPCO advised me that:

> The TAP also bring benefit in clarifying the technology in relation to capabilities which gives JCs and inspectors confidence in understanding what the public authorities are doing when deploying their capabilities. This in turn means a JC can properly scrutinise applications because they will understand the full extent of a capability.[419]

9.20 Dr Glover described the IPCO model, including the capacity for provision of independent technical advice, as representing the 'gold standard'. He also said the calibre of its members is 'impressive'.[420] I agree and in my view the TAP represents best practice in this area.

The United Kingdom TAP represents best practice in the provision of independent technical advice.

416 Investigatory Powers Commissioner (UK), *Annual Report of the Investigatory Powers Commissioner 2023* (Report, 20 December 2024) 22 [5.9].
417 IPCO Technical Advisory Panel (UK), *Technology Advisory Panel Working Protocol* (Document, January 2022) 1.
418 IPCO Technical Advisory Panel (UK), *Proportionality Aide-memoire: Privacy Intrusion in Data Collection and Analytics* (Document, 24 November 2022) 2; Technology Advisory Panel, IPCO, *AI Proportionality Assessment Aid* (Document, 17 April 2025).
419 Email from IPCO to INSLM, 25 July 2025.
420 Philip Glover, *Submission 8*, 4.

9.21 The United Kingdom TAP model can be feasibly implemented in Australia. Provision has recently been made for the appointment of an expert panel for review relating to cyber incidents in another context.[421] Narelle Clark, CEO of the Internet Association of Australia, said that there are a number of similar expert working groups advising government, and they operate very effectively.[422] Even though law enforcement applications of technology may be specialised, the underlying standard protocols are well understood by 'good seasoned industry professionals.'[423] Similar to the United Kingdom TAP, such a body should access diverse experience with a mix of industry professionals and academics.[424] IPCO has published guidance about the way the TAP operates and the experience it expects appointees to have.[425] This should be taken into account in formulating an Australian equivalent.

Recommendation 8: The warrant issuing system also requires:

(a) A mechanism for access to independent technical advice.

...

9.22 I see no reason why, in the interests of the efficiency, a technical advisory panel should not be utilised for other similar purposes. For example, it could assist oversight and review bodies, such as the IGIS and the Ombudsman, that deal with advanced technology. Where relevant to a particular review, it could also assist the Monitor and the Australian Law Reform Commission.

Duty of candour should be legislated

9.23 Access by issuing authorities to complete and accurate information forms a fundamental component of an effective warrant issuing system.

9.24 AFP and ACIC, like state police, have internal controls to ensure the accuracy of warrant applications. For example, ACIC said that they have mandatory annual training that 'addresses legal requirements, privacy considerations and ethical responsibilities' and applications for electronic surveillance warrants must be reviewed by ACIC's legal and compliance teams. Subsequently, 'the ACIC's compliance team, in conjunction with officers responsible for the warrants, ensures

421 *Cyber Security Act 2024* (Cth) s 70; *Cyber Security (Cyber Incident Review Board) Rules 2025* (Cth); Revised Explanatory Memorandum, Cyber Security Bill 2024 (Cth) 8–9 (role of 'Expert Panel').
422 Narelle Clark, CEO, IAA, *Public hearing transcript*, 19 February 2025, 33 [25].
423 Narelle Clark, CEO, IAA, *Public hearing transcript*, 19 February 2025, 34–5. See also Ms Siew Lee Seow, AIIA, *Public hearing transcript*, 19 February 2025, 35.
424 Narelle Clark, CEO, IAA, *Public hearing transcript*, 19 February 2025, 33 [25]–[35].
425 IPCO, Technical Advisory Panel Working Protocol, March 2019 (updated January 2022).

reporting, record keeping, storage, destruction, retention and other legislative and policy obligations are upheld.'[426]

9.25 Internal controls are important and must be retained. However, these policies and procedures are ultimately a matter of administrative discretion, are subject to change and vary between agencies.[427]

No clear common law duty of candour for warrants in Australia

9.26 The duty of candour is a longstanding and well-understood standard for disclosure in court proceedings.[428] The duty is particularly strong for *court* orders that are sought without notice, where 'the moving party is required to point out any salient matter which might tell against the granting of relief.'[429] Broadly, this requires both avoiding any misrepresentation of your own case as well as actively highlighting things that may go against your position.

9.27 However, as discussed earlier, in Australia warrants are *administrative* in character. Even if they are issued by a judge, the judge issues them in a 'personal capacity', so the warrants do not automatically attract safeguards that go with court proceedings.

9.28 Since the decision in *Lego Australia Pty Ltd v Paraggio*,[430] the Full Federal Court has consistently held that applicants for warrants face no general law duty of candour.[431] Non-disclosure issues in the warrant context have been approached through the more confined lens of matters that may vitiate the (administrative) decision of the

426 ACIC, *Submission 17*, 9.

427 For example, in Victoria Police, policy requires applications for surveillance devices be reviewed by Victorian Government Solicitor's Office. We did not identify any equivalent for AFP or ACIC.

428 *Thomas A Edison Ltd v Bullock* (1912) 15 CLR 679, 681–2 (Isaacs J). As Campbell CJ said in *Re South Downs Packers Pty Ltd* [1984] 2 Qd R 559, '[w]hat is material in any case depends, in the first instance, upon the nature of the case sought to be made out and, to that end, must be viewed in the context of all the relevant circumstances': 560. Also see *Lamb v Ariss* [2006] FCA 582, [24] (Sundberg J) citing *Milcap Publishing Group AB v Coranto Corporation Pty Ltd* (1995) 32 IPR 34, 35 (Davies J).

429 *Shinetec (Australia) Pty Ltd v The Gosford Pty Ltd* [2024] NSWCA 174 [51] (Ward ACJ, Leeming and Kirk JJA); *Young v Cooke* [2017] NSWCA 33, [27] (Gleeson JA, Macfarlan JA agreeing) citing *Thomas A Edison Ltd v Bullock* (1912) 15 CLR 679, 681–2 (Isaacs J); *Aristocrat Technologies Australia Pty Ltd v Allam* (2016) 90 ALJR 370.

430 (1994) 52 FCR 542.

431 In *Flanagan v Commissioner of the Australian Federal Police* (1996) 60 FCR 149, the Full Federal Court considered whether there was a duty of candour in respect of applications for warrants under s 46 of the *TIA Act*. After discussing *Karina Fisheries Pty Ltd v Mitson* (1990) 96 ALR 629 and *Lego Australia Pty Ltd v Paraggio* (1994) 52 FCR 542 (*Lego Australia*), the Full Court (Beaumont, Ryan and Lindgren JJ) stated that '[t]he history of this area tends to support the view that there is no general duty of disclosure imposed on the applicant agency otherwise than by the legislative scheme of the statutory code.' See also *Carmody v MacKellar* (1997) 68 FCR 265, 149; *Caratti v Commissioner of the Australian Federal Police* (2017) 257 FCR 166 [32]–[33]; *CXXXVII v Justice White* (2020) 274 FCR 170.

issuing authority: namely, fraud or misrepresentation[432] or want of good faith.[433]

9.29 The absence of a clear and strong duty of candour can be contrasted with the United Kingdom, Canada and New Zealand where a strong duty based on ex parte applications applies (see Annex B for comparisons).

No express statutory duty at Commonwealth level

9.30 At the Commonwealth level, there is no express statutory requirement in the *SD Act* or *Crimes Act* that imposes a duty of candour on warrant applicants. There are offences for *knowingly* giving misleading information where that information is provided in compliance with a law of the Commonwealth.[434] This is a lower standard than a positive duty of candour which would include recklessly providing false or incomplete information. [435]

9.31 I find the absence of a statutory duty of candour for Commonwealth warrant applications surprising, especially as there is such a duty in at least New South Wales, Queensland and Victoria. In those jurisdictions there are specific statutory obligations of disclosure that apply to law enforcement warrant applications. In the case of Queensland and Victoria, this applies to information provided to the public interest monitors. [436]

The requirement for candour is lower at the Commonwealth level than it is in a number of states and in comparable overseas jurisdictions.

[432] Using the language of Beaumont and Whitlam JJ in *Lego Australia.*

[433] Using the language of Hill J in *Lego Australia.*

[434] *Criminal Code* ss 137.1, 137.2.

[435] For example, in Victoria, s 12C(2) of the *Surveillance Devices Act 1999* (Vic) provides that the applicant must not knowingly or recklessly fail to comply with the relevant statutory duty of disclosure.

[436] In Victoria, the applicant must fully disclose to the PIM all matters of which they are aware that are adverse to an application for a surveillance devices warrant or interception warrant: *Surveillance Devices Act 1999* (Vic) s 12C and *Telecommunications (Interception) (State Provisions) Act 1988* (Vic) s 4B. In Queensland, a surveillance device warrant application must fully disclose all matters of which the applicant is aware, both favourable and adverse to the issuing of the warrant: *Police Powers and Responsibilities Act 2000* (Qld) s 328(4). For telecommunications interception warrants, the obligation applies to disclosures to the PIM: *Telecommunications Interception Act 2009* (Qld) s 8. In New South Wales, a surveillance device warrant application must include any information known to the applicant that may be adverse to the application, or if no adverse information is known, a statement to that effect: *Surveillance Devices Act 2007* (NSW) s 17(3)(g).

9.32 The absence of a strong duty of candour should not be taken to mean that AFP and ACIC do not nevertheless act as though such a duty does exist. Indeed, in the public hearing both gave evidence that this was their practice.[437]

Problems have arisen with candour in other jurisdictions

9.33 The experience of other Five Eyes countries is that the duty of candour is not always satisfied in warrant applications. In New Zealand, Canada, the United Kingdom and the United States there is public reporting of detailed reviews which have found failings in this regard. Recent reports and decisions are summarised in Annex B. Noting this overseas experience, it would be prudent to take steps to avoid such problems arising in Australia in the future, including by introducing a statutory duty of candour.

9.34 IGIS and the Ombudsman have done routine inspections of relevant *SLAID Act* warrant applications, but neither the IGIS nor the Ombudsman has undertaken a targeted review focused on the duty of candour of the type described in the overseas examples. IGIS indicated that, if a relevant oversight agency examines warrant applications and supporting affidavits (and, if available, ministerial reports) and identifies any 'red flags' for matters of legality or propriety, it may request further information.[438]

9.35 At this stage, IGIS has not identified a need to undertake a more comprehensive review of standards of disclosure, noting it would be very resource intensive and IGIS has a broad range of oversight responsibilities across a number of agencies. IGIS noted that the introduction of a legislated obligation to observe candour in the process of obtaining a warrant would give an additional 'legality' context to inspections of the relevant agencies' activities.[439]

9.36 The Ombudsman indicated that the introduction of a statutory duty of candour would promote further transparency and enable the Ombudsman to provide a higher level of assurance to the Parliament and the public regarding the use of these powers.[440] As noted in Chapter 16, the Ombudsman's inspection function for *SLAID Act* warrants is currently overly prescriptive. The Ombudsman should have a broader mandate to conduct inspections to look at issues akin to those that the Ombudsman can examine in investigations.

437 Ian McCartney, Deputy Commissioner, AFP, *Public hearing transcript*, 20 February 2025, 32 [15]; Heather Cook, CEO, ACIC, *Public hearing transcript*, 20 February 2025, 57 [10]–[25].

438 This might include asking to be provided with copies of intelligence reports underpinning the matters asserted in the affidavit: IGIS and INSLM, *Agreed Record of Meeting* (28 February 2025) 2.

439 IGIS also stressed that, if the legislation were to be amended as proposed, IGIS would concern themselves with the question whether agencies had been conscious of, and made every reasonable effort to comply with, the duty when preparing their material in support of warrants: IGIS and INSLM, *Agreed Record of Meeting* (28 February 2025) 3.

440 Letter from Ombudsman to INSLM, 31 March 2025.

9.37 At the public hearing, representatives of the Law Council of Australia, Lloyd Babb SC and Tim Game SC, both agreed that an express statutory requirement for disclosure of all material facts would be a significant improvement to the warrant issuing system. In practice, it is very unlikely that the sufficiency or accuracy of information in support of a warrant will be challenged in subsequent legal proceedings.[441] In the context of covert *SLAID Act* warrants, Tim Game SC underlined the importance of ensuring 'strong incentives for truth telling' in the warrant issuing system. Lloyd Babb SC said this will enable the issuing authority to be in a position to assess whether there has been 'full disclosure of both the strengths and weaknesses' contained in a warrant application.[442]

> Absence of a statutory duty of candour for warrant applications is a gap in the current legislation.

441 Even where the validity of a warrant is subject to collateral challenge in subsequent legal proceedings, collateral review is limited to examining the validity of the warrant on its face and would not extend to examining the sufficiency of the material supporting the warrant application: *Ousley v The Queen* (1997) 192 CLR 69, 80 (Toohey J), 85 (Gaudron J), 100 (McHugh J), 130–1 (Gummow J).

442 Tim Game, Law Council, *Public hearing transcript*, 19 February 2025, 49 [35]; Lloyd Babb, Law Council, *Public hearing transcript*, 19 February 2025, 50 [10].

Scope and nature of the duty

9.38 The proposed duty of candour should be similar to that which applies to ex parte proceedings.[443] If Commonwealth PIMs are to be introduced, the same duty should extend to disclosures to the PIM.

9.39 The exact wording for a new express duty of candour is a matter for drafters, but the Queensland model provides a good starting point:

- Applications for the issue of a surveillance device warrant must fully disclose all matters of which the applicant is aware, both favourable and adverse, related to the issuing of the warrant.[444]
- There is a similar obligation to fully disclose to the PIM favourable and adverse matters related to the issuing of relevant warrants.[445]

Recommendation 8: The warrant issuing system also requires:

…

(b) A statutory duty of candour requiring disclosure of all matters of which the applicant is aware, both favourable and adverse.

…

9.40 Any noncompliance would be, at the very least, a matter of serious misconduct. That is likely to be sufficient to ensure that it is taken seriously by applicants.

9.41 Enacting a duty of candour in statute also provides a clear and certain benchmark for retrospective oversight and proactive guidance by the issuing authority or Commonwealth PIM.

9.42 In the United Kingdom, IPCO has set out its expectations in administrative guidance about the information to be disclosed in a warrant application. This includes matters like the potential degree of collateral intrusion on persons not subject to investigation, 'any credible information…which suggests that the person is not, in fact, a legitimate subject of interest' and 'any other factor which materially weakens the case for the warrant, authorisation or notice of which they are aware.' Additional justification is required in cases where 'novel' or 'contentious' activities are sought to be authorised where the meaning of the law is unclear. The New Zealand Inspector-General of Intelligence and Security has also provided guidance that the duty of candour requires disclosure of matters such as the likelihood of intercepting

443 That is, the party seeking an ex parte order fails 'unless he supplies the place of the absent party to the extent of bringing forward all material facts which that party would presumably have brought forward in his defence to that application': *Young v Cooke* [2017] NSWCA 33 [27] (Gleeson JA, Macfarlan JA agreeing) citing *Thomas A Edison Ltd v Bullock* (1912) 15 CLR 679, 681–2 (Isaacs J).

444 *Police Powers and Responsibilities Act 2000* (Qld) s 328(4).

445 *Telecommunications Interception Act 2009* (Qld) s 8.

privileged communications and where a known purpose in seeking the warrant is to share information with third parties. [446]

9.43 I envisage that in the Australian context, the head of the panel of retired judges (Chapter 7) may fulfil a similar role in providing proactive guidance to warrant applicants about their expectations in addressing the duty of candour. Oversight findings of non-compliance with the duty may, through the feedback loop discussed in Chapter 8, lead to certain types of applications being subject to greater scrutiny.

9.44 I considered whether introducing a statutory duty of candour would create a new ground for challenging warrants of a type that would lead to valuable evidence being excluded. It might, but the likelihood is very low given that the practical possibility of challenging covert warrants is already very low. Also, although it is a lower standard, warrants can already be challenged on the basis of (administrative law) judicial review.[447] If the duty of candour is to apply beyond *SLAID Act* warrants to all warrants, the risk of challenge increases but, if warrants are truly infected by a lack of candour then a challenge is justified. However, even if lack of candour is identified, it does not always follow that evidence is excluded.[448]

Need for independent allocation of applications

9.45 Each ART Registry in Australia is set up differently for managing warrant requests. For example, in Sydney, administrative arrangements have been made so that members are rostered and police can book timeslots without knowing who the 'duty' issuing authority is. But in smaller registries police can approach a member directly and ART has limited oversight of personal capacity functions.[449]

9.46 I understand the same situation is true for warrants issued by judges in their personal capacity – police can approach a FCFCOA judge's chambers directly to request a warrant.[450] Because of the federal structure of criminal law in Australia, arrangements for magistrates are likely to vary between jurisdictions.

9.47 In small jurisdictions such as the Australian Capital Territory, there are very few eligible judges or ART members available to issue warrants. Currently, there are only

446 IPCO, *Advisory Notice 1/2018: Approval of Warrants, Authorisations and Notices by Judicial Commissioners* (Document, 8 March 2018) 1 [1]; Office of the Inspector-General of Intelligence and Security (NZ), *Annual Report 2018-2019* (5 November 2019) 9.

447 *Lego Australia* 555–6; *Caratti v Commissioner of the Australian Federal Police* (2017) 257 FCR 166, 180 [34], 182 [37].

448 See *Bunning v Cross* (1978) 141 CLR 54 and equivalent provisions in uniform evidence legislation – see, for example, *Evidence Act 1995* (Cth) s 138.

449 ART and INSLM, *Agreed Record of Meeting* (17 March 2025).

450 Email from Judicial Registrar to INSLM, 22 July 2025.

2 ART members and 2 judges in the Australian Capital Territory authorised to issue NAWs and DDWs.[451]

9.48 Based on the warrants examined for this review, it appears that, for whatever reason, all ACIC warrants and extensions have been issued by one individual ART member.

9.49 Aside from truly urgent situations, no matter how capable individual issuing authorities are and how strong the case for a warrant is, any system that allows those seeking a warrant to decide who they will ask to consider their warrant application is flawed. Warrant applications, like applications to any court or tribunal, should be allocated by a third party like a registry or independent secretariat.

> Allowing those seeking a warrant to decide who they will ask to consider their application undermines public confidence in the independence and rigour of the system and is not best practice.

9.50 Allowing authorities seeking a warrant discretion to select who is asked to issue it is also not consistent with best practice in building anti-corruption measures into the system.[452] Numerous people and groups consulted in this review raised concerns – for example:

- The Law Council of Australia expressed concern that *SLAID Act* warrants 'are effectively authorised by a very narrow pool of eligible ART members' and that 'there is a real risk that 'public confidence in the independence and rigour of the warrant authorisation process will be undermined.'[453]
- ART said it is of concern that this may result in police being able to select which member issues warrants and that in some smaller jurisdictions one member may be the primary or even sole issuer of warrants.[454]

9.51 As highlighted by former Monitor Dr Renwick in an earlier review, the ad hoc character of *persona designata* decision-making constrains the ability of issuing

451 Email from AGD to INSLM, 12 March 2025. Data sourced from *Register of Authorised Persons for Warrants and Other Functions* under ss 12 and 13 (respectively) of the *SD Act* as at 11 March 2025.

452 For example, there is a real risk of increased risks of perceived conflict of interest in smaller jurisdictions with a narrow pool of issuing authorities. The National Anti-Corruption Commission has recently observed that conflicts of interest, whether real, potential or perceived, are 'a significant reputational risk to Commonwealth agencies, and lie at the heart of many forms of corrupt conduct': National Anti-Corruption Commission, *Integrity Outlook 2022/23* (Report, 2023) 17. More generally, relevant international agreements highlight the need to strengthen integrity in relation to assignment of cases: *United Nations Convention against Corruption*, opened for signature 31 October 2003, 2349 UNTS 41 (entered into force 14 December 2005) (Australia ratified and acceded on 7 December 2005) art 11; United Nations Office on Drugs and Crime, *The United Nations Convention against Corruption Implementation Guide and Evaluative Framework for Article 11* (Document, March 2015) 45–6.

453 Law Council, *Submission 23*, 32 [107].

454 ART and INSLM, *Agreed Record of Meeting* (17 March 2025) 2.

authorities to build up expertise on technical matters.[455] This would include the kinds of techniques used in *SLAID Act* warrants. AFP said that 'current eligible ART members … are increasingly familiar with the issuing requirements and technical aspects for consideration.'[456] However, there are ways to ensure expertise in the issuing authority that do not involve police or criminal intelligence agencies being free to choose to take applications to certain individual issuing authorities. These include having a group of dedicated retired judges as issuing authorities supported by PIMs, a technical advisory panel and ongoing professional development.

9.52 The most practical solution to the risk of any perceived (or actual) 'forum shopping' for an issuing authority would seem to be that allocation of warrants and rostering of 'duty' issuing authorities is managed by an independent secretariat.

Recommendation 8: The warrant issuing system also requires:

…

(c) That warrant applications are independently allocated to issuing authorities.

…

9.53 Different mechanisms are in place for emergency situations where is it not possible to contact an issuing authority (see Chapter 13).

Who should manage the system?

9.54 Having established that a new system for issuing intrusive warrants such as *SLAID Act* warrants should be based on a panel of retired judges, PIMs and independent technical advisors, there is a question of whether a new statutory body is needed to 'house' and operate this system.

9.55 Key functions for supporting the system for issuing warrants include:

- independent allocation of warrants to decision-makers
- rostering of issuing authorities
- centralised case management and tracking of applications
- accurate data collection.

455 James Renwick, former Independent National Security Legislation Monitor, *Trust but Verify: A Report Concerning the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 and Related Matters* (Report, 9 July 2020) 36–7 [1.59]–[1.59] (see also Recommendation 4); James Renwick, 'The Role of Courts in National Security Law and Policy, Some Current Issues' (Conference Paper, Australian National University National Security College Conference Securing Our Future, 10 April 2024) 3–4.

456 AFP, *Submission 18*, 9 [53].

9.56 In addition, the secretariat, with direction from the individuals appointed to lead the issuing authorities and PIMs, should coordinate professional development opportunities for issuing authorities and PIMs. The secretariat would also provide general administrative support (booking flights, meeting rooms, security procedures, coordinating ICT and so on).

9.57 Centralised case management of warrant applications has the potential to both significantly enhance reporting and the efficient disposition of warrant applications. In the United Kingdom, in 2022, IPCO implemented improvements to their 'bespoke case management system' in relation to communications data authorisations. IPCO noted that these changes 'have already been beneficial in minimising the number of avoidable errors and have contributed to increasing our efficiency.'[457]

9.58 Improved data collection will also enhance the rigour of public reporting. For example, as discussed in Chapter 15, currently it appears there are inconsistent ways of recording when an application for a warrant has been 'refused.' A denial of a warrant might be counted as a 'refusal' in some jurisdictions, while in others police are given the opportunity 'withdraw' an application that is not accepted or to 'defer' and return with additional information, which avoids it being classed as a refusal.[458] Data collection and reporting, including on the number of warrants considered, granted and refused, should also be a function of the secretariat.

9.59 Broadly there are 3 options for a body to manage warrant issuing: create a new independent body; merge the function with an existing independent body; or have an administrative secretariat of Australian Public Service (APS) staff provided by a department.

Costs associated with a separate statutory body

9.60 Creating a separate statutory body that is responsible for managing the process of issuing warrants is an option. Any new statutory body would have significant financial overheads.[459] Small statutory authorities can be inefficient in the sense that any separate public sector entity attracts all of the statutory obligations and practical requirements (such as human resources, payroll, facilities management and so on) of much larger entities.

9.61 I agree with AGD that 'there would be significant practical challenges in maintaining an independent body that considers only the small number of SLAID warrant applications made each year.'[460] The administrative arrangements would be more efficient if the new issuing arrangements applied to all warrants. However, even then, it would be a small body.

9.62 It could be argued that there would be a greater *perception* of independence from ministers and the executive if the body was a separate entity. However, it is the

457 Investigatory Powers Commissioner (UK), *Annual Report of the Investigatory Powers Commissioner 2022* (Report, 24 November 2023) 32 [7.14].

458 Public reporting in the *SD Act* is based on statistics submitted by police and criminal intelligence agencies, not an independent secretariat.

459 'Types of Australian Government Bodies', *Department of Finance* (Web Page).

460 AGD, *Submission 20*, 9.

decision-making on warrants which needs to be independent, and there are other mechanisms for protecting that independence without creating a new body. The Monitor, for example, is an independent statutory officer not subject to ministerial direction on what they recommend or how they go about conducting reviews.[461] Another example is the recently established Anti-Slavery Commissioner.[462] These statutory appointees have independence in key decision-making and are ably supported by a secretariat drawn from the APS and other government agencies. A separate statutory body is not necessary for independence of decision-making about warrant applications.

A separate statutory body is not necessary for independence of decision-making.

Merging functions with existing statutory bodies

9.63 For the reasons already discussed in Chapter 7, adding management of warrant issuing by retired judges to the workload of ART or a court is unlikely to be efficient or welcome. If ART members no longer issue warrants then there is no basis for believing it would be efficient for the ART to manage a national system for issuing warrants. It is true the ART has a national 'footprint' but so do other agencies and departments including AGD and Home Affairs.

9.64 In the United Kingdom, IPCO has functions beyond authorising warrants. IPCO also inspects the way warrants are executed – a role performed by IGIS and the Ombudsman in Australia. IPCO also independently authorises access to communications data – something that ASIO and police self-authorise in Australia. It is not common internationally to combine issuing and review, although by all accounts it works well in the United Kingdom.

9.65 A significant benefit of the United Kingdom system is that the 'feedback loop' from oversight to issuing authorities can occur internally and the judicial commissioners are also supported by in-house lawyers. The United Kingdom TAP is also integrated into the same agency. This no doubt brings efficiencies.

9.66 Altering the Australian system to reflect IPCO would be a major change to our oversight arrangements (and, if included, communications data access arrangements). In effect, it would require merging the warrant issuing functions with the law enforcement oversight functions of the Ombudsman and some or all of the functions of IGIS. If this type of change were to be made in Australia, careful and specific review and consultation would be required. It was beyond the scope of this review to do that.

461 The Monitor may be referred matters relating to counterterrorism or national security by the Prime Minister, the Attorney-General or the PJCIS. The Prime Minister may give the Monitor directions about the order in which he or she is to deal with references: *INSLM Act* ss 6–7A.

462 *Modern Slavery Act 2018* (Cth) pt 3A.

Combining oversight and authorisation into a single body (like in the United Kingdom) would be a major change and cannot be recommended at this time.

9.67 A very significant improvement can be made to the current system for issuing warrants without altering how existing oversight bodies are structured. If a major review of oversight architecture is required, that is a matter for government to consider and initiate in future. It need not determine (or delay) improvements to the system for issuing warrants.

Should there be a secretariat rather than a separate body?

9.68 An alternative to creating a new statutory body or merging the issuing of warrants with the functions of an existing body or bodies is to rely on a secretariat drawn from a department (most likely AGD). This would seem to be the most efficient option.

9.69 The challenge in secretariat duties, especially managing a roster and allocating warrants to PIMs and issuing authorities, should not be underestimated. In the United Kingdom there are presently 15 judicial commissioners (including the Investigatory Powers Commissioner) who between them manage around 9,500 warrants and around 3,200 targeting decision reviews as well as assisting with inspections. Within IPCO 9 staff have duties that relate directly to supporting the judicial commissioners.[463] However, this is not a direct comparison, because under the IPCO model the judicial commissioner role is integrated into the overall work of IPCO.

9.70 Ultimately, the exact size and constitution of the secretariat will depend on whether the proposed improvements to the system for issuing warrants are applied to all electronic surveillance warrants as well as *SLAID Act* warrants. I do not make a specific recommendation as to whether support for the new system for issuing warrants should be 'housed' in an independent body or be supported by staff made available from a department. What is important is that there is a secretariat of some sort with sufficient size and authority to support the system for issuing warrants.

463 Email from IPCO to INSLM, 25 July 2025. Also see Investigatory Powers Commissioner (UK), *Annual Report of the Investigatory Powers Commissioner 2023* (Report, 20 December 2024) 89 [Table 14.2] (Breakdown of authorisations, notifications and refusals, including those considered by a judicial commissioner).

Recommendation 8: The warrant issuing system also requires:

(a) A mechanism for access to independent technical advice.

(b) A statutory duty of candour requiring disclosure of all matters of which the applicant is aware, both favourable and adverse.

(c) That warrant applications are independently allocated to issuing authorities.

(d) An effective secretariat should be established with functions that include the allocation of warrants, case management and data collection.

9.71 Whether the proposed Commonwealth PIMs (who will likely be independent statutory officers) also rely on the secretariat is a matter to be considered based on both efficiency and the need for independence. On the face of it, having the same secretariat support for both PIMs and issuing authorities would probably be the most efficient model. However, it is important that PIMs have a clear degree of independence and are not, for example, departmental officials.

Resourcing the new system

9.72 To be effective, the warrant issuing system need to be adequately resourced. It is not a function of the INSLM to review resourcing.[464] But, in closing this Part, I note that the Australian Institute of Criminology recently estimated that serious and organised crime cost Australia up to $68.7 billion in 2022–23.[465] The combined budget of AFP and ACIC for 2025–26 is around $2.6 billion.[466] Whatever the ultimate cost of Commonwealth PIMs, retired judges as issuing authorities, a technical advisory panel and a secretariat is, it would be a tiny fraction of this. The covert powers employed law enforcement and criminal intelligence agencies depend on warrants like those in the *SLAID Act*. Those powers are expensive to build, staff and utilise. Public confidence and social licence in such powers depends on the adequacy of the system and its safeguards. The cost of resourcing a small secretariat, PIMs and issuing authorities needs to be assessed in this context.

Public confidence and social licence in covert powers depends on the adequacy of the system and its safeguards. Resourcing should be seen in this context.

464 *INSLM Act* s 6(2)(a).

465 Russell Smith, *Estimating the Costs of Serious and Organised Crime in Australia, 2022–23* (Statistical Report No 50, Australian Institute of Criminology, 19 December 2024) 2.

466 Total agency resourcing for AFP for 2025–2026 is $2,209,976,000; total agency resourcing for ACIC for 2025–2026 is $359,822,000. The total is $2,569,798,000: see Australian Government, *Budget 2025–26 – Agency Resourcing* (Budget Paper No 4, 25 March 2025) 35–6.

Part 4. Definitions, issuing criteria and life cycle of data

Earlier Parts of this report have described the need for AFP and ACIC to have access to special powers in the form of *SLAID Act* warrants, subject to the implementation of a better system to authorise the use of those powers. The report now turns to important definitions demarcating the scope of *SLAID Act* powers and the things the issuing authority must consider in deciding whether to issue a warrant.

This Part examines the offences for which *SLAID Act* warrants are, and should be, available. Currently, the warrants are available for offences punishable by 3 or more years imprisonment as well as some lower offences. This threshold is not consistent with the initial justification for *SLAID Act* powers, and is too low for such significant and invasive powers. The bar should be raised to offences punishable by at least 5 years imprisonment.

When an issuing authority is considering an application for a warrant, they are guided by statutory issuing criteria. The current provisions are inconsistent and unnecessarily complex. They should be replaced by an overarching requirement to be satisfied that the warrant is necessary and proportionate to permit the proposed activity in all the circumstances. To guide the issuing authority and to help shape warrant applications, there should be a succinct non-exhaustive list of the key things to be considered.

Traditionally, the process for balancing the invasion of privacy and the need for police and intelligence agencies to investigate crime has been almost entirely focused on regulating the moment of collection. Because of the volume of data that can now be collected (especially under NAWs), the process for analysing that data and the way in which data can be retained and shared, it is necessary to consider the whole life cycle of data – safeguards for privacy and other rights need to be in place for more than just collection. Also, special safeguards are needed to protect particularly sensitive categories of information. Many of these can be managed through internal policies as long as the issuing authority has regard to the adequacy of these policies when issuing a warrant. There is also scope for some form of published ministerial guidelines or binding administrative guidance on some subjects.

The provisions that deal with when *SLAID Act* warrant information can be disclosed are so complex as to be almost impenetrable. The rules are also inconsistent, and in a few places too restrictive. The disclosure provisions need to be replaced. Unauthorised disclosure should remain an offence, but for the most part there should be reliance on the general secrecy offences in the *Criminal Code.* Limits on the use of NAW information, including its use as evidence, should remain; however, exceptions are needed – for example, to ensure exculpatory material can be disclosed. An exception is also required to ensure that a person can seek legal advice on an assistance order.

Chapter 10: Key definitions

10.1 There are several definitions that are critical to understanding the scope and effect of *SLAID Act* powers. 'Relevant offence', 'computer' and 'criminal network of individuals' are key terms that are discussed in this chapter.

10.2 Changes are recommended to increase the threshold for 'relevant offence' to 5 years. While the definitions of 'computer' and 'criminal network of individuals' are very broad, there is little scope to materially narrow the definitions without compromising the effectiveness of warrants. Instead, other safeguards should be used to ensure that warrants are appropriately targeted – for example, improvements to issuing arrangements (Part 3) and issuing criteria (Chapter 11).

Relevant offences

10.3 *SLAID Act* warrants can be sought in relation to a 'relevant offence.'[467] Broadly speaking, this is any offence punishable by 3 or more years imprisonment, with the following qualifiers.

- For DDWs and NAWs, 'relevant offence' includes additional specific offences with a lower penalty.[468] Further offences (with any penalty) can be prescribed by regulation.[469]
- For ATWs, a 'relevant offence' must also involve or be 'of the same general nature' as any one of a long list of matters (which seems to cover most serious crime types).[470] Additional matters can be prescribed by regulation.[471] Beyond these matters, a number of offences are identified as falling within the definition.[472]

467 *Crimes Act* s 377UK (definition of 'relevant offence'), 3ZZUN(1); *SD Act* ss 6 (definition of 'relevant offence'), 27KA(1), 27KK(1). Both definitions of 'relevant offence' are limited to Commonwealth offices and state offences that have a federal aspect. The PJCIS described the respective definitions as 'materially the same': *PJCIS SLAID Report*, 78 [4.38].

468 *SD Act* s 6 (definition of 'relevant offence' paras (c)–(db)). For example, various offences and former offences against the *AntiMoney Laundering and CounterTerrorism Financing Act 2006* (Cth), the *Fisheries Management Act 1991* (Cth) and the *Torres Strait Fisheries Act 1984* (Cth) for which the maximum penalty is a fine or a shorter term of imprisonment.

469 *SD Act* s 6 (definition of 'relevant offence' para (e)). As at 29 May 2025, no regulations have been made.

470 *Crimes Act* ss 3ZZUK (definitions of 'relevant offence', 'serious Commonwealth offence', 'serious State offence that has a federal aspect') 15GE(2), (4). Some crime types, such as secrecy offences, may not currently be covered.

471 *Crimes Act* s 15GE(2)(zc). As at 29 May 2025, no regulations had been made for this purpose.

472 *Crimes Act* s 15GE(3).

10.4 These definitions of 'relevant offence' existed in the *SD Act* and the *Crimes Act* before the *SLAID Act* was enacted. In neither case was the existing definition modified to account for the specific features of DDWs, NAWs or ATWs.

10.5 The breadth of the definition of 'relevant offence' was a key issue in this review. There were a range of views on the appropriateness of the existing definition and what an alternative may be. Four potential models emerged from submissions and consultation:

- leave the definition unchanged[473]
- include a comprehensive list of which offences the powers can be used for, with or without the ability to add specific offences by regulation[474]
- rather than list specific offences, have a list of 'crime types' and allow the use of the powers for any offence in those categories[475]
- describe 'relevant offence' by reference to the maximum penalty applicable to the offence.[476]

10.6 Each approach has advantages and drawbacks.

Leave definition unchanged

10.7 The current definition has 2 main drawbacks. The first is that the various exceptions and extensions make it complex. Complexity reduces the understandability and clarity of the law. Ad-hoc changes can lead to unexpected omissions from coverage.[477] Undue complexity can also lead to an increased risk of errors in warrant applications. There are times when complexity in law is difficult or impossible to avoid, but in such cases there should be a good reason for the intricacies, and there is no such reason here. This links to the second problem with the current definition: the definition 'piggybacks' on a definition originally set for much less invasive and unusual warrants.

473 Philip Glover, *Submission 8*, 5–6; Uniting Church in Australia, Synod of Victoria and Tasmania, *Submission 14*, 2.

474 Brendan Walker-Munro, *Submission 3*, 9; QCCL, *Submission 6*, 7.

475 Suggested by submitters in combination with a higher penalty threshold: HRLC, *Submission 5*, 9–10; Digital Rights Watch, *Submission 22*, 5–6.

476 QCCL, *Submission 6*, 7 (suggested in the alternative); AJF, *Submission 7*, 7; Joint Academic Submission, *Submission 15*, 5; AHRC, *Submission 21*, 5; Law Council, *Submission 23*, 41 [144]–[145]. Some submissions suggested a combination of a higher threshold and an offence category limiter – for example, HRLC, *Submission 5*, 9; Digital Rights Watch, *Submission 22*, 5.

477 For example, it appears that secrecy offences are not a 'crime type' covered by the definition of 'relevant offence' in *Crimes Act* s 15GE(2) even though secrecy offences in the *Criminal Code* can carry a penalty of up to 10 years imprisonment. Similarly, 'hate crimes', which were recently added to the *Criminal Code* and have penalties of up to 7 years, are not listed.

10.8 The case for *SLAID Act* powers being reserved for especially serious crime types was strongly made in this review, and it is how their intended use was described in the original explanatory materials. This is not currently reflected in the legislation. As an example, the current inclusion of fisheries-related offences for which the penalty is a fine or a short sentence of imprisonment is not consistent with the extraordinary nature of *SLAID Act* powers.

The current approach to defining 'relevant offence' is complex and does not set the bar high enough for the use of extraordinary powers.

Comprehensive list

10.9 The Queensland Council for Civil Liberties submitted that the definition of 'relevant offence' should 'be referable to the specific and heinous crimes that the *SLAID Act* was introduced to combat.'[478]

10.10 A comprehensive list does provide certainty, and theoretically it would enhance transparency by identifying specific offences for which the powers are available. However, these advantages may not be realised in practice. It is likely that the list would be lengthy and would grow over time, particularly if combined with reliance on a regulation-making power.[479] This would make the legislation complex, and members of the public would be less able to readily understand the scope of the powers. There is also a real risk that the list would not be kept up to date, and new relevant serious offences may potentially not be added in a timely way.

In practice, a comprehensive list of relevant offences would be lengthy and complex and could easily become out of date.

10.11 A variation on a comprehensive list is to allow the list (or additions to it) to be contained in regulations. Dr Brendan Walker-Munro suggested that relevant offences could be set out in regulations made under the existing provisions:

> Not only is the use of Regulations to set the boundaries of *SLAID Act* offences already supported by existing legislation, but the use of Regulations issued by the Minister will retain and protect the 'operational flexibility' called for by the Department of Home Affairs in their submissions to Parliament.[480]

478 QCCL, *Submission 6*, 7.

479 See, for example, *TIA Act* s 5D which currently runs to a little over 7 pages long.

480 Brendan Walker Munro, *Submission 3*, 9, citing Home Affairs, Supplementary submission No 9.1 to PJCIS, Parliament of Australia, *Review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (23 April 2021) 6–7.

10.12 Calls for 'operational flexibility' in setting the boundaries of extraordinary police and criminal intelligence powers should be approached with caution. The fact that regulations can be disallowed does provide for some parliamentary oversight, and this is important. However, there is a larger question that this review provides the opportunity to address: what is the minimum level of criminal harm or damage that extraordinary powers like those in the *SLAID Act* should be available for?

Calls for 'operational flexibility' in setting the boundaries of extraordinary police and criminal intelligence powers should be approached with caution.

10.13 The 'minimum bar' for the use of extraordinary powers should be set in legislation. Adding new offences by regulation would undermine this if it allowed 'lower' offences to be added. Allowing new offences to be added by regulation, even if they must be above a minimum threshold, is likely to lead to complexity, inconsistencies and anomalies over time.

List of 'crime types'

10.14 An alternative to listing specific offences is to include in the definition a list of 'crime types.' For example, the Human Rights Law Centre suggested that, in addition to containing a heightened severity qualifier, the definition should contain a 'category qualifier' requiring that relevant offences relate to 'specific serious subject matter.'[481] Digital Rights Watch suggested a similar approach – it recommended the definition include 'a description or list of the nature and seriousness of relevant offences that are intended to captured.'[482]

10.15 A thematic approach risks uncertainty about whether conduct falls within a prescribed category. To reduce that risk, it is foreseeable that the 'crime types' may end up being described so broadly that they would capture less serious offences and/or cover almost all Commonwealth offences. For example, at the moment, issuing authorities are required to give weight to whether the conduct being investigated falls into a list of categories of crimes and crime types – that list covers almost all offences in the *Criminal Code* and offences of a similar type in other Acts.[483] Similarly, the current list of 'matters' for which an ATW can be issued is around 30 items long and would appear to cover most Commonwealth crime types.[484] As outlined above, there is also the risk that any list may contain inadvertent gaps or not be kept up to date.[485]

481 HRLC, *Submission 5*, 9–10.
482 Digital Rights Watch, *Submission 22*, 5–6.
483 *Crimes Act* s 3ZZUP(2)(a), 3ZZUP(3); *SD Act* ss 27KC(2)(a), 27KC(3), 27KM(2)(a), 27KM(2A).
484 *Crimes Act* s 15GE(2).
485 Brendan Walker-Munro, *Submission 3*, 9.

10.16 AFP warned that 'restricting powers to specific crime types may result in AFP's ability to investigate a major incident being limited'.[486]

> A thematic approach risks uncertainty and, based on current practice, would probably eventually end up resulting in a lengthy list covering an excessive number of offences.

Maximum penalty as the threshold

10.17 The Parliament determines how serious different types of criminal conduct are by setting the maximum penalty applicable for the relevant offence. There is some attraction to the simplicity and certainty of setting the threshold for the use of invasive powers by reference to the same measure. Most submitters favoured this approach, although the Australian Human Rights Commission and many non-government groups who supported this approach argued for an increase in the current threshold.[487]

10.18 The current general 3-year threshold is low. It is significantly lower than the 7-year general threshold in the *TIA Act* and the 5-year threshold recommended for electronic surveillance powers in the 2019 Comprehensive Review.[488] For the reasons discussed in Chapter 2, *SLAID Act* powers are distinct from general electronic surveillance powers in the things they authorise (DDWs and ATWs) or breadth of what can be collected (NAWs). In my view it is not appropriate that these significant powers be used for relatively minor offending.

10.19 As a practical matter, a direction from the Attorney-General and AFP operational prioritisation model means that AFP focuses its activities on certain priority areas to 'maximise impact on the criminal environment.' This relevantly includes transnational and serious organised criminal activities that affect Australia and protecting Australians from cybercrime.[489] AFP gave evidence that it has not used any *SLAID Act* warrants for offences punishable by fewer than 5 years imprisonment.[490] Similarly, ACIC operations and investigations are focused on serious organised crime.[491] ACIC advised no NAWs had solely been sought for an offence punishable

---

486 AFP, *Submission 18*, 10 [59].

487 HRLC, *Submission 5*, 9–10; AJF, *Submission 7*, 7; Joint Academic Submission, *Submission 15*, 5; AHRC, *Submission 21*, 5 [12]-[14]; Digital Rights Watch, *Submission 22*, 5–6; Law Council, *Submission 23*, 41. QCCL recommended that the threshold be raised only if its primary recommendation to list specific crimes is not accepted: *Submission 6*, 7.

488 *2019 Comprehensive Review* vol 2, 310 (Recommendation 87). The definition of a 'serious offence' in section 5D of the *TIA Act* applies a 7-year penalty threshold and then creates extensive exceptions for various offences with lower maximum penalties: Law Council, *Submission 23*, 40 [143] (footnote 127).

489 Attorney-General (Cth), *Ministerial Direction (Australian Federal Police): Australian Federal Police Act 1979*, 20 October 2023, 1–2.

490 Mr Ian McCartney, Deputy Commissioner, AFP, *Public hearing transcript*, 20 February 2025, 29.

491 *ACC Act* ss 4 (definition of 'relevant crime'), 7A, 7C; ACIC, *Annual Report 2023-24* (Report, 31 October 2024) 5.

by fewer than 5 years imprisonment, although warrants which were for more serious offences have also listed related 3-year offences.[492]

10.20 There is inevitably some arbitrariness in determining where the threshold should be when it is based on number of years. During this review, potential thresholds of 5 and 7 years were tested against the actual and likely circumstances in which the use of *SLAID Act* powers would be necessary and proportionate.

10.21 Given the nature of *SLAID Act* powers, particularly DDWs, there is an argument for a high threshold for their use.[493] Seven years is a high threshold and is currently used in the *TIA Act*. However, when looking at the cyber-enabled and cyber-dependent crime types for which *SLAID Act* warrants are well suited, there are some offences, such as use of a carriage service for violent extremist material, that would be excluded if a 7-year threshold was set.[494] Some of the other crimes that *SLAID Act* warrants have been used for fall into the 5–7-year maximum penalty range (see Table 3 in Chapter 4).

10.22 A penalty of up to 5 years imprisonment is a significant penalty. After considering the types of offences this would capture, I am satisfied that this threshold would appropriately limit the use of DDWs, NAWs and ATWs to circumstances where it would be proportionate to use such significant powers, while also ensuring that these tools remain available for the most serious types of offending that AFP and ACIC are targeting.

A penalty of up to 5 years imprisonment is a significant penalty.

10.23 There is a question about whether there should be specific exceptions to the general 5-year penalty threshold, such as where lower level offending is known to be linked to further (but not yet specifically identifiable) and more serious conduct; or to include specific offences that, due to their nature, are difficult to investigated in any other way.[495]

492 Wendy Darling, National Manager, ACIC, *Public hearing transcript*, 20 February 2025, 48; INSLM, *Summary of private hearing – ACIC*, 11 March 2025 1. In a private hearing this matter was explored further with ACIC and the Monitor noted that there is nothing preventing ACIC 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: INSLM, *Summary of private hearing – ACIC*, 11 March 2025, 2.

493 QCCL, *Submission 6*, 7; AHRC, *Submission 21*, 5 [12]–[14].

494 An offence under *Criminal Code* sch 1 s 474.45B carries a penalty of imprisonment for 5 years, as does an offence under s 474.45C, 'Possessing or controlling violent extremist material obtained or accessed using a carriage services'.

495 See, for example, Matthew Rippon, Deputy CEO, ACIC, *Public hearing transcript*, 20 February 2025, 48–9; INSLM, *Summary of private hearing – ACIC*, 11 March 2025, 2.

10.24 No compelling case has been put to me, including in the evidence advanced in private hearings, for any exceptions to a 5-year penalty threshold as a limit on the use of *SLAID Act* powers. An offence penalty threshold without exceptions would present a clear, bright line limiting the use of these extraordinary powers and avoid the kind of definitional complexity that has crept into existing electronic surveillance legislation.

> The kind of definitional complexity that has crept into existing electronic surveillance legislation should be avoided.

10.25 Allowing for exceptions that are bespoke for *SLAID Act* powers is also likely to compound the existing complexity that has arisen because of differences in offence thresholds for the use of covert powers more generally. Examining the inconsistencies between similar definitions of 'relevant offence' for electronic surveillance powers, the 2019 Comprehensive Review recommended that a new electronic surveillance Act should provide for a unified 5-year offence threshold. The government agreed to this recommendation.[496] Both the Law Council and AGD echoed this recommendation in submitting to the present review that definitions such as 'relevant offence' and 'serious offence' should be aligned across the Commonwealth legislative framework for electronic surveillance powers.[497]

10.26 Alignment with other electronic surveillance powers is not a reason in itself to adopt a 5year penalty threshold, given the special features of *SLAID Act* powers. However, I consider it more appropriate for these special features to be addressed through other mechanisms, including the new safeguards recommended in this report, where (unlike 'relevant offence') considerations specifically to do with the proportionality of DDWs, NAWs and ATWs can be introduced. If the additional safeguards recommended in this report, relating to issuing of warrants (recommendations 6-8) and issuing criteria (recommendations 12-13), are introduced; then I recommend that the definition of 'relevant offence' for *SLAID Act* powers be set at offences with a maximum penalty of 5 years imprisonment or more. If the other recommendations are not accepted then a 7year penalty would be more appropriate without those additional safeguards.

> **Recommendation 9: Warrants should only be available for offences punishable by 5 or more years imprisonment.**

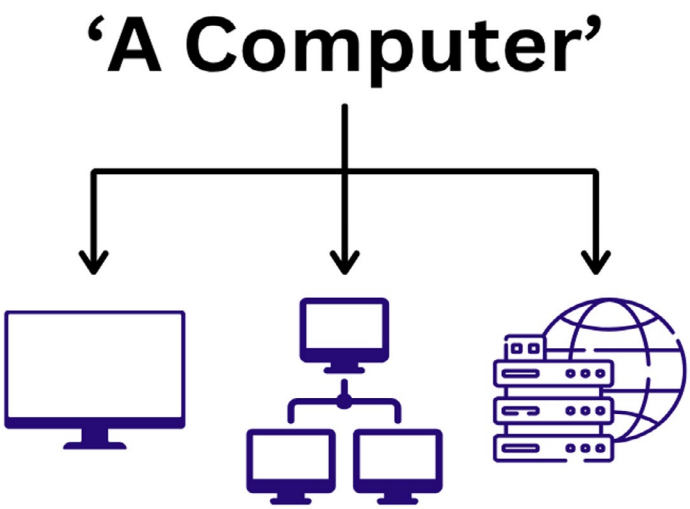
496 *2019 Comprehensive Review* vol 2, 310 (Recommendation 87); Government response to the *2019 Comprehensive Review*, 26. It was also recommended that offences should only be included as exceptions to the 5-year threshold for surveillance if they are punishable by at least 3 years imprisonment and the use of electronic surveillance powers is necessary to effectively investigate the offences: *2019 Comprehensive Review* vol 2, 315 (Recommendation 89), agreed in principle by government: Government response to the *2019 Comprehensive Review*, 27.

497 AGD, *Submission 20*, 14–15; Law Council, *Submission 23*, 40–41 [142]–[145] (Recommendation 14).

Computer

10.27 The definition of 'computer' is a key aspect of *SLAID Act* warrants because all of them authorise what would otherwise be unlawful access or disruption to data on 'a computer' or the use of 'a computer' to facilitate access to a targeted account.[498] The definition of 'a computer' extends significantly beyond a single standalone device and includes multiple computers, computer systems and computer networks.[499] Given that most computers are connected to the internet or some other form of network, the number of computers that might be covered by a single warrant is extraordinarily large.[500]

Figure 3 – Definition of 'a computer'



The definition of 'a computer' is extraordinarily broad.

10.28 Civil society groups and the Australian Human Rights Commission argued that this definition is excessively broad and suggested mechanisms for greater specificity in the definition, including separating out more restricted definitions of 'computer,' 'computer system' and 'computer network.'[501] The Australian Human Rights Commission said that '[t]hese distinctions would ensure that a warrant targeting a

498 *Crimes Act* s 3ZZUR(2)(b)(i); *SD Act* ss 27KA(1)(b)–(c), 27KE(2), 27KK(1)(b), 27KK(7), 27KP(2)(c).

499 'Computer' means all or part of (a) one or more computers; or (b) one or more computer systems; or (c) one or more computer networks; or (d) any combination of the above: *Crimes Act* s 3ZZUK (definition of 'computer'); *SD Act* s 6 (definition of 'computer').

500 The ordinary meaning of 'computer' includes things like modern mobile phones: see *Commissioner of the AFP v Luppino* (2021) 284 FCR 233.

501 Joint Academic Submission, *Submission 15*, 6–7. AHRC, *Submission 21*, 7 [19]–[23].

'computer' does not unintentionally extend to an entire corporate network or cloud infrastructure.'[502]

10.29 AGD said that it was necessary to include multiple computers in the definition of 'computer', as it is 'vital to disrupt serious criminal activity.' It argued the definition should include 'cloud-based servers, virtual machines … and distributed file systems.'[503] AGD also noted that the current definition of 'computer' aligns with the definition under the Council of Europe *Convention on Cybercrime*[504] and 'reflects a broad international consensus among Parties to the Convention as to the need for powers used to investigate cyber-dependent and cyber-enabled crime to reflect the evolution of networking and computing technologies.'[505] AFP gave evidence that a 'significant challenge when it comes to cybercrime' is that the distributed nature of computing enables offending to 'scale very quickly and very easily,' such as by use of 'bot-nets' that can infect 'potentially hundreds, if not thousands or tens of thousands of Australians' home computers and mobile phones' to facilitate further offending.[506]

10.30 I understand, and share, concerns such as those raised by numerous submitters, including the Australian Human Rights Commission, joint academic submitters and the Queensland Council for Civil Liberties, about the breadth of the definition of 'computer.'[507] I also recognise that modern computing is highly distributed and that data which may be an appropriate target for *SLAID Act* warrants is likely to be spread across multiple devices, computers, servers, systems and networks. It would be extremely difficult to narrow the definition of 'computer' without risking unintentional limits on the proper use of powers. To resolve this dilemma, it is necessary to consider whether other safeguards in the system can adequality protect against overly broad warrants. This is not an issue confined to *SLAID Act* powers, as the definition of 'a computer' is based on pre-existing definitions in the *SD Act* and *Crimes Act*.[508] Similar definitions exist in other Acts that permit surveillance.[509]

> The definition of 'computer' needs to recognise the distributed nature of modern computing and be understood in the context of existing and proposed safeguards.

502 AHRC, *Submission 21*, 7 [22].
503 AGD, *Submission 20*, 15.
504 *Convention on Cybercrime*, opened for signature 23 November 2001, [2013] ATS 9 (entered into force 1 July 2004) art 1 (definition of 'computer system') (*Convention on Cybercrime*).
505 AGD, *Submission 20*, 16.
506 Rob Nelson, Commander, AFP, *Public hearing transcript*, 20 February 2025, 23–4.
507 QCCL, *Submission* 6, 7–8; Joint Academic Submission, *Submission 15*, 6–7; AHRC, *Submission 21*, 7 [19]–[23]. See also Digital Rights Watch, *Submission 22*, 4.
508 *Crimes Act* s 3ZZUK (definition of 'computer'); *SD Act* s 6 (definition of 'computer'). The Joint Academic Submission argued for a consistent narrowing of this definition in relation to all warrant powers picking up this definition: Joint Academic Submission, *Submission 15*, 6–7.
509 *ASIO Act* s 4 (definition of 'computer'). The *TIA Act* also contains provisions reliant on the definitions of 'computer' in the *SD Act* and *ASIO Act*.

10.31 In the context of *SLAID Act* powers, there are several provisions that should operate to limit to some extent which computers can be targeted in practice including those listed below.

- In the case of DDWs and NAWs, the issuing authority must be satisfied of the proportionality of the warrant, which would include the nature of the relevant 'computer' to be targeted:[510]
  - in the case of DDWs, the warrant must specify the details of and associated with the computer to be targeted[511]
  - in the case of NAWs, the warrant authorises the doing of things in relation to the relevant *target* computer. The target computer must be a computer used by, or likely to be used by, one or more of the individuals in the 'criminal network of individuals.' Although details of the computer are not required to be specified in the warrant, the network is.[512]
- For ATWs, the authority to use a computer is limited to the purpose of taking control of the account or accounts covered by the warrant.[513]

10.32 These existing additional provisions provide some comfort. However, they rely on the issuing authority having enough accurate information and technical expertise to understand the full breadth of what authorising access to 'a computer' will mean in practice. For the reasons discussed in Part 3 I am not satisfied that our current warrant-issuing system is set up to achieve this.[514]

10.33 Rigorous oversight is also critical. To facilitate oversight, there should be reporting on which *computers* were accessed under the warrant. Where that cannot be ascertained, the warrant report should explain why this is the case. Over time, oversight bodies will no doubt build their technical capabilities, and access to independent technical advice will enhance their ability to inspect and review operations.[515] Under the proposals in Chapter 8, the outcomes of those inspections will form part of independent submissions to issuing authorities to inform their consideration of proportionality and whether conditions are required on future warrants.

If recommendations 6-8 and 12-13 are adopted then the existing broad definition of a 'computer' should remain.

510 *SD Act* ss 27KC(1)(b), 27KM(1)(aa). Recommendation 12 in Chapter 11 will require that an overarching test of necessity and proportionality apply to *SLAID Act* warrants, including ATWs.
511 *SD Act* ss 27KD(1)(b)(iv)–(vi).
512 *SD Act* ss 27KK(1)(b), 27KN(1)(b)(iii).
513 *Crimes Act* s 3ZZUR(2).
514 See also recommendations in Chapter 11 to make requirements as to proportionality and privacy clearer. For DDWs this includes being clear that they are a warrant of 'last resort.'
515 Consider, for example, the way that IPCO inspectors currently utilise access to independent technical advisors in the course of warrant inspections. See further, Chapter 16 on oversight.

Criminal network of individuals

10.34 NAWs can be sought in relation to a 'criminal network of individuals.' This key concept is defined in s 7A of the *SD Act*.[516]

10.35 In essence, a 'criminal network of individuals' is a group of people who are using the same electronic service and that service enables at least one individual in the group to engage in or communicate about a relevant offence; or to facilitate or communicate about facilitating another person (whether in the group or not) engaging in a relevant offence. It is immaterial whether the identities of the individuals in the group or details of offences can be ascertained, and the composition of the group can change from time to time.[517]

10.36 There is no doubt that this is a broad definition. There are a great many ways that very large numbers of individuals might be 'electronically linked' through some 'electronic service' or 'electronic communication.' For example, it could be argued that all individuals using the same social media platform or messaging app would fall within the definition as that those platforms and apps probably enable at least some people to engage in, or facilitate, crime or to communicate about facilitating crime. This breadth appears to be intentional: the Revised Explanatory Memorandum gave the examples of WhatsApp and Telegram when describing the concept of electronically linked individuals.[518]

10.37 Many non-government submissions expressed concern about the broad nature of the definition and the risk of inadvertently collecting data about innocent third parties. For example, the Australian Human Rights Commission said that the 'expansive scope' of the definition 'risks violating the privacy of innocent parties and undermines the rule of law by allowing covert and intrusive surveillance measures to target individuals without evidence or reasonable suspicion of their individual involvement in unlawful conduct.'[519]

---

516 Regard also needs to be had to terms within the definition which are separately defined, including 'electronically linked group of individuals' and 'electronic communication'. *SD Act* s 6 defines 'electronically linked group of individuals' to mean a group of 2 or more individuals, where each individual in the group does, or is likely to, use the same electronic service as at least one other individual in the group; or communicate with at least one other individual in the group by electronic communication. 'Electronic service' is defined by reference to pt 15 of the *Telecommunications Act 1997* (Cth) and means a service (with some exceptions) that allows end-users to access material using a carriage service or a service that delivers material to persons having equipment appropriate for receiving that material, where the delivery of the service is by means of a carriage service. Many of the terms in that definition are further defined, making it a particularly complex definition.

517 *SD Act* ss 27KK(2).

518 Revised Explanatory Memorandum 80–81 [398]–[399].

519 AHRC, *Submission 21*, 6 [17]. See also HRLC, *Submission 5*, 9, noting this broad reach presented an outsized risk to the work of both journalists and whistleblowers, and Brendan Walker-Munro, *Submission 3*, 6 describing the definition as 'extremely broad.'

Can the definition be narrowed?

10.38 The majority of civil society submitters and the Australian Human Rights Commission supported narrowing the scope of the definition of 'criminal network of individuals' to require proof of a common purpose or nexus between the suspected conduct of an individual group member and the actions or intentions of the group as a whole.[520] This 'common purpose' is consistent with the approach in the United Kingdom, where the subject of a targeted interception or examination warrant may be, among other things, 'a group of persons who share a common purpose or who carry on, or may carry on, a particular activity.'[521]

10.39 Evidence of at least a reasonable suspicion that a person is engaged in unlawful activity may be an appropriate standard for ordinary surveillance warrants. However, a NAW is not an ordinary surveillance warrant. Its purpose is different and it has some additional safeguards – with more to be added if the recommendations of this review are accepted.

10.40 In this context and with these additional safeguards, I am not satisfied that proof of a common purpose would be an appropriate issuing criterion for NAWs. The NAW is intended to have utility at an early stage of an investigation where the identity of members of a group involved in serious criminal activity are unknown. I agree with AGD that any amendment to the definition must still allow AFP and ACIC to continue to 'gather intelligence about potential facilitators and those that may be unknowing participants in criminality.'[522]

10.41 I considered recommending restricting the breadth of the concept of 'criminal network of individuals' by establishing 2 types of NAWs with distinct issuing criteria reflecting the risk of collateral impact on individuals not suspected of being involved in criminal activity. This would be consistent with the 2019 Comprehensive Review's point about the need for an additional criterion for group warrants and the additional criterion currently imposed in relation to 'B-party' interception warrants.[523] I tested this proposal in consultations, private hearings and at the public hearing.

10.42 AGD submitted that strengthened safeguards should not 'inadvertently introduce legal uncertainty about the rules.'[524] AFP and ACIC accepted that warrants need to be appropriately targeted but argued that the breadth of the definition remains necessary for current and proposed operations. ACIC said that 'without the breadth of the definitions and the current threshold for access, in many instances, ACIC would not have been able to identify the offending given the way TSOC

520 Law Council, *Submission 23*, 41–2 [146]–[150] (the Law Council also recommended related changes to the issuing criteria: *Submission 23*, 42); AHRC, *Submission 21*, 6. HRLC and the joint academic submitters agreed and made a similar recommendation: HRLC, *Submission 5*, 9–10; Joint Academic Submission, *Submission 15*, 7. Dr Walker-Munro supported an approach analogous to that taken in the United Kingdom under the *Investigatory Powers Act 2016* (UK) in relation to certain thematic warrants: *Submission 3*, 7–8.

521 *Investigatory Powers Act 2016* (UK) s 17(2)(a). See Law Council, *Submission 23*, 23 [71].

522 AGD, *Supplementary submission 28*, 12.

523 *2019 Comprehensive Review* vol 2, 292 (Rec 82); T*IA Act* ss 9(1)(a)(ia), 9(3), 46(1)(d)(ii), 46(3).

524 AGD, *Supplementary submission 28*, 12.

networks segment and anonymise their activities.'[525] AFP said that the current definition 'provides appropriate breadth to enable the targeting of individuals involved in the commission of relevant offences,' allows AFP to 'collect intelligence on multiple concurrent users of electronic services and communication platforms' and 'accounts for the diverse and changeable nature of criminal network of individuals.'[526] I am also cognisant that, due to changes in the way criminals use technology, there is likely to be an increasing focus on commercially available platforms used by a range of persons who are not subject to investigation in the future.[527]

Little scope to meaningfully narrow the definition

10.43 I have concluded that having 2 types of NAWs would introduce unnecessary complexity. Furthermore, I am satisfied that there is limited scope to meaningfully narrow the definition of 'criminal network of individuals' without compromising the effectiveness and purpose of NAWs. Reliance must instead be placed on other safeguards – for example, retaining the limitation that NAW information cannot be used as evidence; and improving the system for issuing warrants so that the issuing authority is in the best possible position to make a well-informed, independent decision on the actual scope of the proposed operation (see Part 3). Importantly, the issuing criteria should require the issuing authority to take into consideration the likely impact on the privacy rights of any person; whether sensitive categories of information are likely to be collected; and, if so, whether there are effective procedures for restricting access and disclosure, including, where feasible, early deletion. These proposed new issuing criteria are discussed further in Chapter 11.

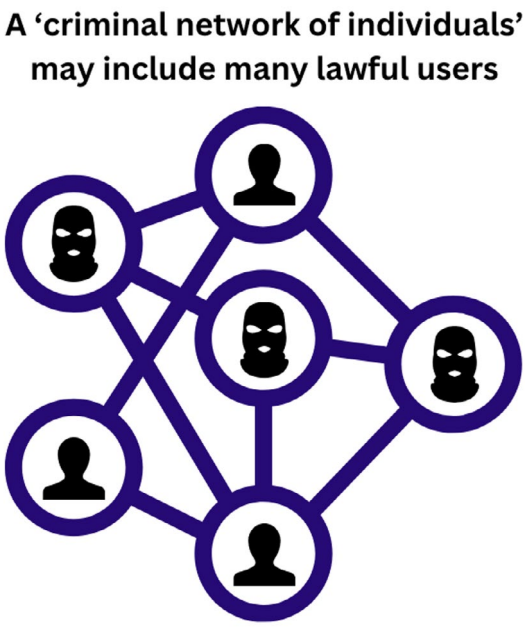
> Subject to implementation of the additional safeguards about issuing arrangements and criteria proposed in Part 3 and Chapter 11, the current breadth of the definition of a 'network' that a NAW can apply to should be maintained.

525 ACIC, *Submission 17*, 4–5.
526 AFP, *Submission 18*, 6 [31].
527 Rob Nelson, Commander, AFP, *Public hearing transcript*, 20 February 2025, 30.

Misleading nature of the label 'criminal network of individuals'

10.44 Although I have found that the current breadth of the 'network' that a NAW can apply to should be maintained, I consider the label 'criminal network of individuals' to be misleading. Use of this phrase implies that all individuals captured by the definition are suspected of committing, or facilitating, a relevant offence. Clearly, that is not a requirement of the definition; many people who could fall within the current definition will not be suspected of engaging in any criminal activity. While changing the label would not in itself change the scope of NAW, this definition plays an important communicative role.

Figure 4 – Definition of 'criminal network of individuals'



10.45 Dr Glover highlighted the difficulty in describing an electronic network as 'criminal.' As Dr Glover said, even with respect to a dedicated encrypted communication device or platform almost exclusively used by criminals, 'the network of criminals are the physical/human users, not the platform.'[528] Dr Glover proposed the use of the term 'network investigation warrant', further submitting that:

> There seems no need to apply the controversial pejorative/prejudicial descriptor 'criminal' at this stage of the intelligence-only surveillance-centred investigation. Reasonable suspicion of involvement in inchoate or complete offending grounds virtually all types of warrant, without needing to pre-judge the targets of the warrant as 'criminal' in either the enabling legislation or the warrant application. Why the difference in this context?[529]

10.46 The risk that the label 'criminal network of individuals' will have a misleading effect is more pronounced given the changing environment in which 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 and platforms.[530] These were to be targeted by ACIC because they are almost exclusively used by serious organised crime groups in order to try to obfuscate criminal activity and identities.[531] In ordinary language, a network of that type could be sensibly described as a criminal network of individuals on the basis that almost everyone using it is suspected of involvement in serious organised crime. But the statutory definition is not that narrow and does not bear much resemblance to the ordinary meaning. Because of successful law enforcement actions criminal groups are losing trust in those types of dedicated devices and platforms and are moving to general platforms used by a wide range of users hoping that their communications can be 'lost in the noise of legitimate users.'[532]

10.47 Unless the definition is narrowed to include reasonable suspicion of criminal activity for all members of the network, the name of this category should be changed. The term 'targeted network' or a similar expression would more accurately describe the broad scope of persons picked up by this concept.

Recommendation 10: The expression 'criminal network of individuals' should be renamed 'targeted network' or something similar that does not misleadingly imply that all persons using the same electronic service are suspected of being engaged in criminal activity.

528 Philip Glover, *Submission 8*, 6.
529 Philip Glover, *Supplementary submission 27*, 2.
530 ACIC, Submission No 23 to PJCIS, *Review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (February 2021) 2.
531 INSLM, *Summary of private hearing – ACIC*, 29 July 2024, 2.
532 Rob Nelson, Commander, AFP, *Public hearing transcript*, 20 February 2025, 30.

Chapter 11: Things to consider when issuing a warrant

11.1 An issuing authority may approve an application for a *SLAID Act* warrant if they are satisfied that relevant criteria have been met. These criteria are supplemented by lengthy lists of matters relevant to, but not necessarily determinative of, the issuing authority's decision. Those relevant matters do not themselves constitute additional issuing criteria or impose strict thresholds on when warrants may be approved, but they do require the issuing authority to 'have regard to' a range of things.

11.2 Some of the warrant criteria are directed towards testing the reasonable suspicion underpinning the warrant application and verifying that, where a warrant is sought in urgent circumstances, it was impracticable to apply in person or with a sworn affidavit. Beyond these matters, the overarching test for positively assessing whether a warrant should be issued ought to be whether it is necessary and proportionate to permit the proposed activity in all the circumstances. To guide the issuing authority and help shape warrant applications, there should be a non-exhaustive list of the key things to be considered.

11.3 Currently, ATWs have no overarching test of necessity and proportionality and DDWs and NAWs express that test differently. For all 3 warrant types, the list of what must be considered is long, overlapping and has some critical gaps. If other safeguards recommended by this review relating to new issuing arrangements and particularly the introduction of PIMs, statutory duty of candour and access to independent technical advice are introduced then the statutory list of matters to be considered can be significantly streamlined.

Issuing criteria

11.4 Currently, for DDWs and NAWs, the key criteria that must be satisfied are broadly that:

- there are reasonable grounds for the suspicion founding the application for the warrant; and
- the thing authorised by the warrant is reasonably necessary (or justified) and proportionate, having regard to the offences to be disrupted or in relation to which information is sought.[533]

11.5 For ATWs, the only criterion the issuing magistrate must be satisfied of is that there are reasonable grounds for the suspicion founding the application for the warrant.[534]

533 *SD Act* ss 27KC(1)(a)–(b), 27KM(1)((a)–(aa).
534 *Crimes Act* s 3ZZUP(1).

Reasonable grounds for suspicion

11.6 To seek a warrant an *AFP or ACIC delegate* must have reasonable grounds for suspecting that the warrant is likely to assist in frustrating the commission of a relevant offence or gathering relevant evidence or intelligence. The threshold is expressed slightly differently for each warrant.

- For DDWs, disruption of data in a computer will *substantially assist in frustrating* the commission of one or more relevant offences which have been, are being, are about to be, or are likely to be committed.[535]
- For NAWs, a group of individuals is a 'criminal network of individuals', and access to data in a computer that is likely to be used by any person in that group will *substantially assist in the collection of intelligence* about the person or group and is relevant to the prevention, detection or frustration of one or more kinds of relevant offence.[536]
- For ATWs, relevant offences have been, are being, are about to be, or are likely to be committed; an investigation is, will be or is likely to be conducted; and taking control of the online account is *necessary* while investigating the commission of relevant offences for the purpose of *enabling evidence to be obtained.*[537]

11.7 The differences in the threshold for suspicion reflect the different purposes for which each kind of power may be sought.[538]

It is appropriate that the issuing authority must be satisfied that there is in fact a reasonable basis for the relevant suspicion founding the application.

Urgent warrants – extra criteria

11.8 Each of the warrants introduced by the *SLAID Act* may be sought remotely or without a sworn affidavit where the applicant believes it is *impracticable* to appear in person or to swear an affidavit before making the application.[539] This 'impracticality' test is one of the things that the issuing authority for DDWs and NAWs must be expressly satisfied of:

(c) in the case of an unsworn application – that it would have been impracticable for an affidavit to have been sworn or prepared before the application was made; and

(d) in the case of a remote application – that it would have been impracticable for the application to have been made in person.[540]

535 *SD Act* s 27KA(1).
536 *SD Act* s 27KK(1).
537 *Crimes Act* s 3ZZUN(1).
538 *Crimes Act* s 3ZZUP(1); *SD Act* ss 27KC(1)(a), 27KM(1)(a).
539 *Crimes Act* ss 3ZZUN(2)(b), 3ZZUN(2B); *SD Act* ss 27KA(4), 27KB(1), 27KK(5), 27KL(1).
540 *SD Act* ss 27KC(1)(c)–(d), 27KM(1)(b)–(c).

Such applications are known as 'urgent' warrant applications.[541]

11.9 The *Crimes Act* does not expressly require the issuing authority to be satisfied of equivalent 'impracticality' criteria for urgent ATWs.

11.10 Applications made without an affidavit also have an 'urgency' test for the applicant. For DDWs this is that *immediate* disruption of the data is likely to substantially assist in frustrating the relevant offences. Similarly, for NAWs, it is that *immediate* access to the data will substantially assist in collecting the relevant intelligence. Urgent ATW applications depend on it being *immediately* necessary to take over the account to enable the relevant evidence to be obtained.[542]

11.11 An issuing authority might interpret the general requirement that they be satisfied of the 'suspicion founding the application' as including the impracticality test for ATWs and the urgency test for all unsworn applications. However, there is no express requirement that an issuing authority be satisfied of the 'urgency' test. This uncertainty is not aided by the drafting, including the different language used for the main criterion ('suspects on reasonable grounds') and the impracticality and urgency criteria ('belief') or the list of things that the issuing authority must take into account (which do not include urgency or impracticality). Although urgent applications are rare, it would be preferable to make clear that, when they are sought, the issuing authority should turn their mind to the existence of a reasonable basis for the applicant's belief in both the impracticality and the urgency criteria.

Recommendation 11: For all urgent applications, the issuing authority should need to be satisfied that there is a reasonable basis for both the 'impracticality' and the 'urgency' criteria.

11.12 I note that adjusting the overarching test for all *SLAID Act* warrants to 'necessary and proportionate in all the circumstances' as recommended below would partially rectify the absence of the urgent warrant criteria in relevant ATW decisions by providing for *consideration* of the urgent circumstances. However, this would still not require the issuing authority specifically to be *satisfied* of the reasonable basis of the applicant's belief in that regard in the way they currently must for NAWs and DDWs.

541 They must be followed by an affidavit/written record within 72 hours: *Crimes Act* s 3ZZUN(2C), (5); *SD Act* ss 27KA(5)(b), 27KK(6)(b). Quaintly, the *Crimes Act* s 3ZZUN(2D) and *SD Act* ss 27KB(2), 27KL(2) refer to transmitting an affidavit by 'fax'. It is time to update this to cover other electronic means.

542 *Crimes Act* s 3ZZUN(2B)(a); *SD Act* ss 27KA(4)(a), 27KK(5)(a).

Necessity and proportionality

11.13 The overarching test for issuing a warrant should be whether it is necessary and proportionate to permit the proposed activity in all the circumstances. For DDWs and NAWs, the *SD Act* contains a test close to this which is set out below.

- For DDWs, the disruption of data must be 'reasonably necessary and proportionate' having regard to the offences to be disrupted.[543]
- NAWs require that the 'issue of the warrant is justified and proportionate' having regard to the 'kinds of offences' in relation to which information will be gathered.[544]

11.14 It is not clear why NAWs use the term 'justified', when DDWs use 'necessary', and if one standard is intended to be lower than the other. The Supplementary Explanatory Memorandum explains that 'necessary' for DDWs is directed towards consideration of 'whether the proposed disruption activity is a reasonable and appropriate means of frustrating [the relevant offence's] commission.'[545] Meanwhile, 'justified' for NAWs is explained to have been 'included to require the issuing of the warrant to be defensible by a reasonable person.'[546] The language 'necessary and proportionate' would be more appropriate for both warrant types as an overarching test capturing all the considerations relevant to issuing decisions. Necessary and proportionate is a well known legal test.

11.15 A revised test of it being necessary and proportionate would be best if it meant *necessary and proportionate in all the circumstances.* This would clearly include having regard to the offences but would also make clear that other considerations are in play.

11.16 Currently, there is no clear overarching necessity and proportionality test for ATWs. Some of the mandatory considerations for ATWs (discussed below) do pertain to proportionality. But these do not strictly require the issuing magistrate be satisfied that taking over the specified account(s) is necessary and proportionate. Such an approach does not constitute or replace the overall assessment of a necessity and proportionality threshold.

There is no clear overarching necessity and proportionality test for ATWs.

543 *SD Act* s 27KC(1)(b).
544 *SD Act* s 27KM (1)(aa).
545 Supplementary Explanatory Memorandum, 17.
546 Supplementary Explanatory Memorandum, 31.

11.17 Relying solely on a list of individual matters to be considered, without an overarching proportionality test, has the potential to limit the factors the issuing authority takes into account and also, as a practical matter, the material put to them. As stated by AFP, 'warrant applications focus on the matters that are required to be considered by the [issuing authority].' Other matters that may go to necessity and proportionality will not necessarily be included in an application.

Recommendation 12: Issuing criteria should require that the issuing authority is satisfied that the warrant is necessary and proportionate in all the circumstances.

...

Key matters to consider when assessing warrant applications

11.18 It is appropriate for the statute to set out key matters that Parliament intends the issuing authority to consider when deciding whether to approve a warrant application. Ideally, this is expressed as a non-exhaustive list focused on what can be expected to be the most important issues.

11.19 The current list of matters to be considered in determining an application is long. For ATWs it runs to around 3 pages of legislation and for NAWs and DDWs it is closer to 4 for each. Some were added during the parliamentary process for the passage of the *SLAID Act*.[547]

11.20 In the current system, where there is no PIM to test applications, the lengthy lists are understandable and possibly necessary. However, the current lists have some gaps as well as some overlaps. This can make warrant applications long and complex and at risk of missing key issues.

547 *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (SLAID Bill), Government Amendment QL187, items (5)–(7), (25)–(29), and (37)–(38). See Supplementary Explanatory Memorandum 2–3 for a summary of the considerations that were introduced to the SLAID Bill by government amendments.

11.21 For example, among the things an issuing authority must 'have regard to' in deciding whether to issue a NAW are:

> (b) the extent to which access to data under the warrant will assist in the collection of intelligence that:
>
> (i) relates to [the target 'criminal network of individuals'] or to any one of the individuals in that group
>
> (ii) is relevant to the prevention, detection or frustration of one of more kinds of relevant offence; and
>
> (c) the likely intelligence value of any information sought to be obtained; and
>
> (d) whether the things authorised by the warrant are proportionate to the likely intelligence value of any information sought to be obtained.[548]

11.22 These are all relevant points, but as drafted they are overlapping. It would be clearer to instead state the overriding considerations that these points are directed towards – in this case, how likely it is that the warrant will result in access to valuable intelligence. An overarching test of necessity and proportionality allows for the issuing authority to consider how such matters, along with the others addressed below, should be applied in the context of the objectives, proposed activities and relevant circumstances of an individual warrant. If PIMs are introduced they can be expected to be a significant aid to ensuring applications address relevant matters and act as a strong safeguard against key points not being raised and tested. See Chapter 8 on the proposed role of PIMs.

11.23 Introduction of the proposed statutory duty of candour will require the warrant applicant to disclose all relevant material, including material that tends against the issuing of a warrant, to both the PIM and the issuing authority. This safeguard will also reduce the need to rely on overly detailed criteria. See Chapter 9 on duty of candour. Access to independent technical advice will improve the issuing authority's ability to independently assess matters such as likelihood of success, feasibility of other methods and risk of damage or loss of property, including infrastructure.

> With new safeguards in other areas, there is scope to reduce the length and complexity of the current list of mandatory considerations.

548 *SD Act* s 27KM(2)(b)–(d).

11.24 Subject to introduction of a statutory duty of candour, PIMs and access to technical advice, there is potential to reduce the non-exhaustive list of matters to be considered when assessing proportionality to 6 key points:

- gravity of the offences being investigated (or, for DDWs, disrupted)
- likelihood that the proposed activity will achieve the warrant objective
- intrusion on the privacy rights of any person
- interference with property, including the introduction of vulnerabilities
- the appropriate protection of 'privileged' and other sensitive information
- whether what is sought to be achieved by the warrant could reasonably be achieved by other, less intrusive means.

11.25 Each of these is discussed below. A seventh consideration specific to applications made remotely or without an affidavit (relating to impracticality and urgency, as discussed above) could either be added to this list or treated as a separate matter for such applications.

11.26 I note that this approach for *SLAID Act* warrants broadly aligns with the suggested approach for assessment of necessity and proportionality across the *SD Act* and *TIA Act* set out in the 2019 Comprehensive Review.[549]

Gravity of the offences being investigated

11.27 The nature and gravity of the offence or offences being investigated needs to be clear in the warrant application and is certainly a key factor. Currently, the requirement to consider the gravity of the offence is described differently for each warrant. In each case, it is spread over several subsections and is in some parts confusing. For example, for an ATW the magistrate must consider the nature and gravity of the offences (s 3ZZUP(2(a)) and must 'give weight to' whether the offences amount to 'an activity' or an offence within the long list in s 3ZZUP(3)(a)–(f), but the magistrate is not prevented from issuing a warrant for offences not covered by that list (s 3ZZUP(5)). The list seemingly covers all offences that AFP or ACIC might be likely to seek a warrant for, including some that do not currently fall into the definition of a 'relevant offence' for the purpose of ATWs.[550] Similar provisions apply to DDWs and NAWs.[551]

549 *2019 Comprehensive Review* vol 2, 284–5 [28.15] (Recommendation 80).

550 For example, the list covers all offences against ch 5 of the *Criminal Code* – which includes secrecy and other offences not covered by the definition of 'relevant offence' in the *Crimes Act*. The list also includes very broad categories such as 'conduct [that] … has the potential to cause a danger to the community' and any 'conduct that involves or is related to transnational crime, or serious crime or organised crime not covered by the [other] paragraphs.'

551 *SD Act* ss 27KC(2)(a), 27KC(3), 27KM(2)(a), 27KM(2A).

11.28 This complexity does not actually add any meaningful safeguard. Increasing the penalty threshold for 'relevant offence' to at least a minimum penalty of 5 years imprisonment, per Recommendation 9, would be a simpler and more effective measure. That does not automatically mean all offences that carry a penalty of 5 years or more should or will justify a warrant – the other factors also need to be considered. PIMs would be well placed to assist issuing authorities to test the way suspected offending is described. With these new measures in place, the existing provisions about the gravity of the conduct being investigated could be simplified to just that: a simple requirement to consider the nature and gravity of the alleged offences being investigated (or, for DDWs, disrupted).

Recommendation 12: In assessing necessity and proportionality, the list of matters to be considered should include the:

(a) nature and gravity of the offences being investigated (or disrupted);

...

Likelihood that the proposed activity will achieve the warrant objective

11.29 Not all warrants will result in valuable evidence or intelligence being obtained. There is inevitably an element of speculation as to what the person or persons suspected of wrongdoing will do or say while under surveillance and what data exists or will be generated during the period of the warrant. In the case of warrants that involve access to data, there is a risk that the information will be unintelligible due to encryption or unobtainable due to security or other measures.[552] But all warrants authorise the State to intrude on the affairs and rights of individuals, potentially including those not suspected of wrongdoing. Thus, one of the factors an issuing authority must weigh is how likely it is the proposed activity will achieve the warrant objective.

11.30 Assessing the likelihood of success requires an understanding of exactly what is proposed, the challenges expected to be faced and broadly how they are to be overcome. Those issuing *SLAID Act* warrants, particularly DDWs, NAWs and covert ATWs, may need a high degree of technical understanding to ensure that they are able to make an independent assessment of likelihood of success. As discussed in Chapter 9, this means they must have access to independent technical advice in some cases. The strength of AFP or ACIC case as to why those computers targeted by the warrant are likely to contain valuable intelligence or evidence of the relevant offences or, for DDWs, result in an effective disruption will also be relevant. Ensuring that warrant applications contain enough information and that it can be tested is a key role of the proposed PIMs (see Chapter 8).

552 AFP said that 'in 2022-2023, 96.1% of AFP's lawfully intercepted content was unintelligible due to encryption.' AFP, *Submission 18*, 3 [15].

Assessing the likelihood of success requires an understanding of exactly what is proposed, the challenges expected to be faced and broadly how they are to be overcome.

11.31 The current provisions on NAWs, DDWs and ATWs more or less require that the issuing authority turn their mind to the likelihood that a warrant will result in valuable evidence, intelligence or disruption. For NAWs and DDWs, this requirement is spread across multiple overlapping provisions and involves assessment of not only the value of the outcome sought by the warrant but also the likelihood that outcome can be successfully achieved.[553]

11.32 For ATWs, the current requirement to have regard to 'the likely evidential value of any evidence sought to be obtained' seems to require an assessment of the admissibility and weight of evidence sought.[554] It is not as obvious that this requires an assessment of how likely it is that AFP or ACIC will be able to take over the account.[555]

11.33 A low likelihood of success will not always mean that a warrant is not issued, particularly if the potential intelligence, evidence or disruption is of high value. The issuing authority should be clearly directed to consider both of these points in assessing whether the proposed activity will meet the warrant objective.

Recommendation 12: In assessing necessity and proportionality, the list of matters to be considered should include the:

…

(b) likelihood that the activity proposed under the warrant will succeed as well as the likely value of the resulting intelligence, evidence or disruption;

…

11.34 Simplification will result in a clearer indication of what is to be considered and less repetition in applications. The safeguard of having PIMs should ensure that sufficient detail is provided and that, where necessary, the issuing authority is encouraged to call on independent technical advice.

553 *SD Act* ss 27KC(2)(b), (ca), (cb), 27KM(2)(b)-(d).

554 *Crimes Act* s 3ZZUP(2)(d).

555 I note that strictly speaking, evidence is not obtained directly through the account takeover itself, but instead by use of other powers such as computer access or search warrants after the account has been taken over: Rob Nelson, AFP, *Public hearing transcript*, 20 February 2025, 34–5. Further, if ACIC ATWs are modified to become intelligence, rather than evidence collection warrants (recommendation 3) a corresponding change to this criterion for ACIC ATWs would be needed.

Privacy and property rights

11.35 The successful use of *SLAID Act* warrants will inevitably have an impact on privacy. Some activities authorised under warrants can also interfere, at least temporarily, with property rights. The interference with these rights is not necessarily limited to the rights of the person or persons suspected of wrongdoing. There is also a risk that there will be more intrusion, interference or disruption than is intended.

Privacy

11.36 Australia's obligations under article 17 of the *International Covenant on Civil and Political Rights* (*ICCPR*)[556] permit invasion of privacy rights where necessary and proportionate for a permitted purpose, including to further the investigation of serious crime. This can include interference with the privacy rights of a person suspected of being engaged in unlawful activity, as well as persons who are not suspected of wrongdoing – provided the test of necessity and proportionality is met in each case. In the context of covert surveillance, article 17 imposes a test of 'strict necessity'[557] (see Chapter 17).

11.37 Currently, ATW provisions direct the issuing authority to have regard to 'the extent to which the privacy of any person is likely to be affected.'[558] However, as noted earlier, ATWs do not have an express requirement to assess necessity and proportionality. As such, it is not completely clear that the ATW provisions satisfy Australia's obligations under article 17.

11.38 NAWs do have an overarching 'justified and proportionate' requirement. However, it is not entirely clear that the choice of the term 'justified' in this context meets the 'strictly necessary' test for the *ICCPR*. Even if it does, the NAW privacy provisions are deficient because they only require consideration of 'the extent to which the execution of the warrant is likely to result in access to data of persons who are lawfully using a computer, and any privacy implications (to the extent known to the eligible judge or AAT member) resulting from that access.'[559]

556 *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) art 17 (*ICCPR*).

557 *Szabó and Vissy v Hungary*, European Court of Human Rights, Application No 37138/14 (2016) 38–9 [73]. The Court held that the test of strict necessity is to be applied in the context of secret surveillance, stating that 'given the particular character of the interference in question and the potential of cutting-edge surveillance technologies to invade citizens' privacy, the Court considers that the requirement "necessary in a democratic society" must be interpreted in this context as requiring "strict necessity".'

558 *Crimes Act* s 3ZZUP(2)(c).

559 *SD Act* s 27KM(2)(f). This requirement was inserted by a government amendment, implementing the recommendation of the PJCIS in part to strengthen oversight: SLAID Bill, Government Amendment QL187, item 26; PJCIS SLAID Report, 146–7 [6.111] Recommendation 31; IGIS, Submission No 18 to PJCIS, *Review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (26 February 2011), 10 [35].

11.39 There are 2 problems with this approach. The first is that it does not require consideration of the privacy of all persons. The second is the caveat 'to the extent know to the [issuing authority].'

11.40 Some might assume that those suspected of committing a crime have no right to privacy, but that is not correct. People are innocent until proven guilty, and suspicion of wrongdoing does not of itself automatically remove rights. Seen through this lens, it is necessary to consider the likely impact of the warrant on the privacy of any person. The weighing of how much invasion of privacy is necessary and proportionate will be affected by the facts of the case, such as how much evidence there is, if any, that a person is involved in wrongdoing, how serious the conduct is, how sensitive the personal information being collected may be, what alternative measures are available and what privacy mitigating steps (including conditions) are being applied. In other words, the stronger the grounds for suspecting a person is involved in serious criminal activity and the more likely that the information will be relevant to this, the easier it is to establish that invasion of their privacy is proportionate.

11.41 As with all warrant applications, the onus should be on the applicant to provide as much relevant information as is known to them at the time, and it is then for the issuing authority to reach a conclusion. The current drafting, which refers to considering privacy 'to the extent known by [the issuing authority],' implies that the onus is somehow reversed. This drafting is at odds with other parts of the issuing criteria, such as the 'existence of alternative less intrusive means,' which is not caveated by 'to the extent known to the issuing authority.' The caveat on privacy may have been an attempt to highlight that it is not possible to know everything before a warrant is issued. If that was the intent, it is unnecessary and the existence of that caveat is, at best, confusing.

11.42 The privacy test for DDWs is substantially the same as for NAWs.[560]

Recommendation 12: In assessing necessity and proportionality, the list of matters to be considered should include the:

...

(c) extent to which the privacy of any person is likely to be interfered with;

...

11.43 Importantly, in considering impact on privacy, the issuing authority should also be able to have regard to what happens to data after it has been collected. This includes consideration of the effectiveness of agency policies and any feedback from oversight agencies on compliance with those policies. In Chapter 12, I recommend that further consideration be given to issuing binding administrative guidance to provide additional protections for the collection, use, retention and

560 *SD Act* s 27KC(2)(cb) requires consideration of the likely access to or disruption of data of persons lawfully using a computer and any privacy implications (to the extent known) arising from that access or disruption.

disclosure of information and particularly personal and sensitive information. Post-collection safeguards are particularly important in demonstrating the proportionality of collecting data on people not suspected of wrongdoing and for special categories of data.

Property-related rights – individuals and infrastructure

11.44 It is clear on the face of the legislation that it has always been understood that *SLAID Act* warrants may result in interference with property-related rights.[561] This is not of itself unusual. Physical search warrants have long authorised what would otherwise be trespass. What is unusual about *SLAID Act* warrants is the type of online interference with rights they permit and the greater potential for interference with the rights of third parties, including those who supply and operate commercial infrastructure. Because the warrants are covert, those affected may not know who has caused damage or interference.

11.45 There are constitutional limits to the kinds of interference with property that can be authorised by Parliament or the executive.[562] This is presumably why DDWs and ATWs may not authorise the permanent loss of money, digital currency or property (other than data).[563]

11.46 Warrants do authorise the interference, interruption or obstruction of the lawful use of a computer (by any person) where it is necessary and proportionate to do so in properly executing the warrant.[564] This is not limited to use of a particular computer or an account by an individual. Interference, interruption or obstruction can extend to commercial infrastructure if it is somehow necessary and proportionate. Submissions to this review raised concerns that the techniques and technologies used to execute warrants may involve introducing or exploiting, without disclosing, a 'systemic vulnerability' and that this could damage the security and reliability of systems, as well as compromise the privacy of individuals using those systems.[565]

11.47 The issuing authority should consider the likelihood of interference (etc.) with lawful use of computers by individuals as well as any risk to commercial infrastructure.

561 *Crimes Act* s 3ZZUR(5), (8); *SD Act* ss 27KE(7), (12), 27KP(6).
562 See, for example, Lael Weis, 'Property' in Cheryl Saunders and Adrienne Stone (eds), *The Oxford Handbook of the Australian Constitution* (Oxford University Press, 2018), 1,013.
563 *Crimes Act* s 3ZZUR(8); *SD Act* s 27KE(12).
564 *Crimes Act* ss 3ZZUR(2)(c)–(d), 3ZZUR(5)(a); *SD Act* ss 27KE(2)(d)–(e), 27KE(7)(a), 27KP(2)(d)–(e), 27KP(6)(a).
565 QCCL, *Submission 6*, 8; Joint Academic Submission, *Submission 15*, 9; IAA, *Submission 16*, 3; Ausma Bernot, Griffith University, *Public hearing transcript*, 19 February 2025, 72. See also Law Council, *Submission 23*, 60–1 [231] mentioning systemic vulnerabilities in relation to availability of technical advice.

11.48 It is a current requirement for DDWs and ATWs that the issuing authority have regard to the extent to which the execution of the warrant is likely to:

- cause a person to suffer temporary loss of money, digital currency or property (other than data)[566]
- result in 'access to or disruption of data' (DDWs) or 'impact on' (ATWs) a person lawfully using a computer.[567]

11.49 For NAWs there is no equivalent requirement to consider loss or disruption.

Recommendation 12: In assessing necessity and proportionality, the list of matters to be considered should include the:

…

(d) extent to which property rights are likely to be interfered with, including through introduction of vulnerabilities;

…

11.50 In using the umbrella term 'property rights' in this recommendation, I intend to also cover the risk of interference with lawful use of a computer, including temporary loss of money (etc.) and the introduction of vulnerabilities. This should be expressed in a way that applies to persons as individuals and persons as corporate entities.

11.51 As with other technical matters, this assessment requires a combination of candour on the part of the applicant and access to independent technical advice where needed. In some cases, this assessment will be straightforward – for example, where an ATW simply authorises changing a password to prevent a person from accessing a personal email account. In other cases, it is potentially a challenging task – for example, understanding how a proposed operation intends to access vulnerabilities of some sort in order to covertly access data not otherwise available.

Should consultation with industry be mandatory?

11.52 Submissions and evidence from industry groups were directed towards ensuring that relevant entities were consulted about the risk of 'technical complications, operational disruptions, and inefficiencies that could otherwise be mitigated through early consultation.'

566 *Crimes Act* s 3ZZUP(2)(db); *SD Act* s 27KC(2)(cd). There are also requirements for agencies to notify the Ombudsman where material or loss or damage has been caused to persons lawfully using a computer in executing a DDW: *SD Act* s 49C.

567 *Crimes Act* s 3ZZUP(2)(da); *SD Act* s 27KC(2)(cb). The ATW requirement is caveated by 'to the extent known by the magistrate', this caveat should be removed (see [11.41] above).

11.53 The Internet Association of Australia suggested new mandatory considerations that require the issuing authority to consider any systemic vulnerabilities that may be introduced as a result of executing *SLAID Act* warrants and that AFP and ACIC be required to 'engage in consultation with the relevant industry entity about the implications of SLAID activity, as far as reasonably practicable.'[568] Evidence was given that this consultation, along with advice to the issuing authority, would '… ensure that any proposed SLAID activities are technically feasible, sound, reasonable, and will not cause unreasonable harms to communications networks or systems, and will not unreasonably curtail users' lawful use …' of digital services.[569] The Australian Information Industry Association submitted that issuing authorities should 'assess whether consultation has occurred, and, if not, whether its absence is reasonable in the circumstances.'[570]

11.54 AGD said that the existing criteria for *SLAID Act* warrants already direct agencies and issuing authorities to consider any potential impact on lawful users.[571] It also said:

> [AGD] is not aware of any significant or systemic issues concerning agencies failing to identify risks to third party systems, or unintended loss or damage to lawful users of systems when exercising SLAID powers, that would require the introduction of a mandatory consultation requirement prior to the exercise of SLAID powers.[572]

11.55 AFP said that it 'assesses the risk of harm to commercial infrastructure and industry to be low' and that '[c]onsultation with industry is always given due consideration prior to the use of intrusive powers.'[573] ACIC provided evidence that it 'performs comprehensive testing before undertaking computer access activities to ensure that risks of technical error are mitigated when such capabilities are used.'[574] Beyond internal technical assessment, AFP indicated that it 'also will engage on occasions and have in relation to these [warrants] with industry to seek their assistance.'[575]

568 IAA, *Submission 16*, 3.
569 Sophia Joo, IAA, *Public hearing transcript*, 19 February 2025, 31.
570 AIIA, *Submission 12*, 3–4.
571 AGD, *Submission 20*, 17.
572 AGD, *Submission 20*, 17–18.
573 AFP, *Submission 18*, 11 [64].
574 ACIC, *Submission 17*, 9.
575 Rob Nelson, Commander, AFP, *Public hearing transcript*, 20 February 2025, 26.

11.56 Even though the risk may be low and not arise often, where there is a possibility that an operation may cause damage or introduce a vulnerability to commercial infrastructure, this should be disclosed in the warrant application. Where this type of risk has been identified and there has not been consultation with industry, it can be expected that, when reviewing the draft warrant application, PIMs will ask why this is the case. If necessary, the PIM might advocate for independent technical advice to be sought. With these additional safeguards in place, a new mandatory consultation requirement is not necessary.

> With the introduction of a statutory duty of candor and access to independent technical advice and PIMs, a *mandatory* industry consultation requirement is not necessary. Consultation would nevertheless be prudent whenever there is a risk to commercial infrastructure or lawful services.

11.57 In reaching this view I have also had regard to schemes for developing and testing new capability, particularly those introduced by the *TOLA Act*.[576] These types of capability development measures can be used for *SLAID Act* warrants and would require consultation.[577] I am also mindful that some *SLAID Act* warrants will be executed using well-established and well-tested technology where repeated consultation is not needed and that there is, as AFP said, a real risk that mandatory requirement to undertake consultation may 'delay law enforcement activity resulting in increased harm to victims.'[578]

11.58 I note AGD's evidence that 'it is not self-evident that companies would be well-placed to provide advice on the potential implications of the exercise of a covert capability with which they may have limited familiarity.'[579]

576 The *TOLA Act* scheme requires consultation with a designated communications provider before a technical assistance notice or technical capability notice can be given (or varied), other than in urgent circumstances or where the provider waives the consultation requirement: *Telecommunications Act 1997* (Cth) ss 317PA, 317W, 317Y.

577 ACIC said it 'plans to use data disruption warrants (DDW) by leveraging Industry Assistance provisions under [the *TOLA Act*]': ACIC, *Submission 17*, 3.

578 AFP, *Submission 18*, 11 [64].

579 AGD, *Submission 20*, 18.

Special categories of information

11.59 Individual privacy and interference with property rights are not the only categories of harm that issuing authorities should consider. In addition to harm to individuals, there is also a risk that warrants can authorise things that interfere with wider public interests or are contrary to the institutions and conventions supporting those interests. For example, there may be circumstances where the warrant is likely to result in access to sensitive categories of information that are usually subject to privileges or heightened confidentiality in other contexts, including those associated with LPP and information about a journalist's sources.[580]

11.60 As discussed in Chapter 12, it is not only the risk of collection of this sort of information that needs to be assessed; the policies and procedures that reduce (or do not reduce) the risk that privileged information will be used, communicated or retained are also relevant.

Legal professional privilege

11.61 Communications made for the dominant purpose of giving or obtaining legal advice, or for use in existing or anticipated litigation, are subject to confidentiality under LPP. The privilege belongs to the client, not the lawyer, and it is among the professional obligations of a lawyer to preserve the confidentiality of information that a client discloses.[581]

11.62 The High Court has emphasised that LPP is essential for the administration of justice, enabling clients seeking legal advice to communicate with candour and honesty:

> The privilege exists to serve the public interest in the administration of justice by encouraging full and frank disclosure by clients to their lawyers… a person should be entitled to seek and obtain legal advice in the conduct of his or her affairs, and seek legal assistance in and for the purposes of the conduct of actual or anticipated litigation, without the apprehension of being prejudiced by subsequent disclosure of the communication.[582]

580 See HRLC, *Submission 5*, 7, 9; QCCL, *Submission 6*, 8; AJF, *Submission 7*, 5–6; Philip Glover, *Submission 8*, 6–7; Joint Academic Submission, *Submission 15*, 10–11; AFP, *Submission 18*, 10 [61]–[62]; MEAA, *Submission 19*, 1–2; AGD, *Submission 20*, 16–17; AHRC, *Submission 21*, 11–12 [36]–[39]; Law Council, *Submission 23*, 5–6 [4]–[6], 44–46 [159]–[165], 57 [216].

581 See, for example, *Legal Profession Uniform Law Australian Solicitors' Conduct Rules 2015* (NSW) r 9. Equivalent obligations apply in each state and territory. See further 'Australian Solicitors' Conduct Rules', *Law Council,* (Web Page, 11 April 2024).

582 *Esso Australia Resources Ltd v Federal Commissioner of Taxation* (1999) 201 CLR 49 [35] (Gleeson CJ; Gaudron and Gummow JJ), citing *Baker v Campbell* (1983) 153 CLR 52, 114 (Deane J).

11.63 There is not currently any express requirement for an issuing authority to consider whether a *SLAID Act* warrant is likely to result in access to material subject to LPP. This may be compared with legislation in other jurisdictions. For example, under the *Investigatory Powers Act 2016* (UK), one of the mandatory considerations when a public authority is deciding whether to issue a warrant is the sensitivity of the information to be obtained, including items subject to LPP.[583]

> Unlike in the United Kingdom, there is no express requirement to consider sensitive categories of information, including LPP.

11.64 When LPP information is collected under a covert surveillance warrant, the *SD Act* and the *Crimes Act* do not abrogate the privilege.[584] Although it is open to a person to make a claim of LPP if the information is used in subsequent proceedings, this is unlikely to be the case with information collected under the *SLAID Act* powers.[585] An additional difficulty is that collecting information that is, or could be, subject to LPP hollows out the practical utility of the privilege because confidentiality is lost.[586]

11.65 The Law Council said that it is 'especially important in the context of covert electronic surveillance that there be clear provisions protecting LPP to support public trust in the independence of the legal profession.'[587] It also argued that information subject to LPP should be subject to 'more stringent issuing criteria' before collection.[588]

11.66 AGD asserted that LPP considerations already form part of the issuing authorities' consideration when determining whether to issue a warrant, and it was open to an issuing authority to impose conditions or restrictions concerning the collection, use or disclosure of privilege information.[589]

583 *Investigatory Powers Act 2016* (UK) s 2(2), (5).

584 AGD, *Submission 20*, 16. Because there are no clear words abrogating LPP, it is assumed that Parliament did not intend to abrogate LPP: see further *Daniels Corporation International Pty Ltd v Australian Competition and Consumer Commission* (2002) 213 CLR 543, 552–3 [9]–[11].

585 This is because, as discussed in Chapter 4, it is unlikely that information collected under a *SLAID Act* warrant will be used in evidence and that DDWs, NAWs and some ATWs are covert.

586 Law Council, *Submission 23*, 46 [166].

587 Law Council, *Submission 23*, 5 [6].

588 Law Council, *Submission 23*, 47 [168].

589 AGD, *Submission 20*, 16. It is not clear on the face of the legislation that LPP is to be an explicit consideration. It is also noted that in my Office's review of *SLAID Act* warrant related documentation, there were no examples of warrants where conditions of any type (other than statutory conditions) were in fact imposed.

11.67 The likelihood of collecting information subject to LPP should be one of the things that the issuing authority specifically considers. The issuing authority should also have regard to agency policies and procedures that dictate what happens to information subject to LPP that has been collected, intentionally or otherwise (see Chapter 12). The adequacy of those policies and the history of compliance with them may be relevant to whether a condition about LPP should be added to a warrant. As outlined in Chapter 8, these latter points are ones that a PIM is well placed to put to the issuing authority.

> Where there is a risk LPP information may be collected, the issuing authority should consider the public interest in maintaining confidentiality in that information.

11.68 I acknowledge the concern raised by the Uniting Church in Australia, Synod of Victoria and Tasmania, about the potential for a person or entity to make an improper claim of privilege over documents so they can evade law enforcement investigations.[590] As a rule underpinned by the interests of efficient administration of justice, LPP will not apply to communications that are not for the dominant purpose of genuine legal advice or litigation. An illegal or improper exertion of the privilege – for example, where documents are communicated to a lawyer with the sole objective of excluding them from an investigation – would not attract confidentiality.[591] In any case, as noted above, it is unlikely a person would be afforded the opportunity to seek to exert privilege over a communication that is the subject of a *SLAID Act* warrant, given their covert nature. My recommendations regarding LPP and the issuing criteria for *SLAID Act* warrants are intended to apply to information clearly subject to LPP or that can reasonably be expected to be subject to LPP.

Journalists

11.69 There is a public interest in having a free press.[592] An essential aspect of maintaining a free press is recognising that journalists need to be able to protect the identity of their sources. This is recognised to some extent in the existing provisions for *SLAID Act* warrants. Under these provisions, the issuing authority is expressly required to consider if the public interest in issuing the warrant outweighs the public interest in protecting the confidentiality of journalists' sources and facilitating the exchange of information with journalists.[593] Similar to the defence for secrecy offences in pt 5.6 of

590 Uniting Church in Australia, Synod of Victoria and Tasmania, *Submission 14*, 3–4.

591 LPP does not apply where a client consults a lawyer in furtherance of a crime or fraud. See *Evidence Act 1995* (Cth) s 125, reflecting the principle in *R v Cox and Railton* (1884) 14 QBD 153. It was noted at the public hearing that this principle introduces complexity where 'a lawyer might not be aware that they are being used for the commission of crime': Tim Game SC, Law Council, *Public hearing transcript*, 19 February 2025, 52–3.

592 AJF, *Submission 7*, 5 [4.1]–[4.4]; MEAA, *Submission 19*, 1. For further discussion of the interest in a free press in the context of secrecy offences, see Jake Blight, Independent National Security Legislation Monitor, *Secrecy Offences – Review of Part 5.6 of the Criminal Code 1995* (Report, 27 June 2024) 21–4 [2.11]–[2.23] (*2024 INSLM Secrecy Review*).

593 *Crimes Act* s 3ZZUP(dc); *SD Act* ss 27KC(ce), 27KM(fa).

the *Criminal Code,* the consideration is limited to persons 'working in a professional capacity as a journalist' (or their employer).[594]

11.70 However, the current protection for journalists' sources (in relation to *SLAID Act* warrants) is only enlivened if *each* of the offences for which the warrant is sought is an offence against a secrecy provision.[595] This is a significant limitation.

> The current protection for journalists' sources is only enlivened if each of the offences for which the warrant is sought is an offence against a secrecy provision.

11.71 It is quite conceivable that, even if a possible breach of a secrecy offence was being investigated, other offences – for example, property theft – would also be being investigated in relation to the conduct under suspicion, meaning the rule would not apply.[596] For ATWs, secrecy offences are not included in the list of offence types that define a 'relevant offence' (see Chapter 10), making it difficult to see how the current requirement has any effect at all.[597] Journalist source information may also be discovered incidentally during an investigation into other offences. For example, if a journalist had a source in an organised crime group, police investigating the crime group may identify the source. Again, the current rule to protect journalists' sources would not apply.

11.72 Both the Alliance for Journalists' Freedom and the Media, Entertainment and Arts Alliance argued that, when deciding whether to grant a warrant likely to collect journalists' information, the issuing authority should have regard to the public interest in matters such as the public's right to know, the protection of journalistic sources, and media freedom.[598]

---

594 The 'journalist defence' for the secrecy offences is actually wider and applies to any person who is 'engaged in the business of reporting news, presenting current affairs or expressing editorial or other content in news media.' See *2024 INSLM Secrecy Review*, 213–4 [9.84]–[9.88].

595 *Crimes Act* s 3ZZUP(2)(dc)(ii); *SD Act* ss 27KC(2)(ce)(ii), 27KM(2)(fa)(ii).

596 For example, in *R v McBride (No 4)* [2024] ACTSC 147 the defendant was charged with theft under pt 7.2 of the *Criminal Code* as well as unlawfully giving or obtaining information as to defences under Part VII of the *Defence Act 1903* (Cth).

597 *Crimes Act* s 15GE(2).

598 AJF, *Submission 7*, 7 Recommendation 6.4; MEAA, *Submission 19*, 1–2. Note that both recommended media organisations themselves be granted a right to appear or be represented to contest a warrant.

11.73 The provisions concerning journalists' sources should be broadened to ensure that, where there is a reasonable possibility that a journalist's source may be identified, the public interest in journalists protecting their sources is considered. As identification of sources may be incidental or unexpected, the issuing authority should also have regard to the adequacy of policies and procedures that are applied if a source or likely source is incidentally identified.

> Where there is a reasonable possibility that a journalist's source may be identified, the public interest in protecting sources should be specifically considered.

11.74 For the reasons discussed in Chapter 8, PIMs should be able to make submissions on warrant applications, including those that may involve a journalist or media organisation. It can, and should, be expected that the public interest in a free press and protecting journalists' sources is something PIMs will be alert to, even where the 'target' of an operation is not a journalists or media organisation and where the crime being investigated is not a secrecy offence. If PIMs are introduced and protection of journalist's sources more generally is an issuing consideration then it seems unnecessary to set up a separate (narrower) special advocate scheme specific to media organisations/ journalists and secrecy offences.[599]

Other special categories of information

11.75 There are times when other special categories of information should form part of a proportionality assessment. Although they may not arise often, other categories include information subject to parliamentary privilege; medical practitioner–patient confidentiality; and biometric information and data about First Nations People and their Country, knowledge and resources.[600]

11.76 As with information about LPP and journalists' sources, those applying for a warrant should identify when it is foreseeable that sensitive categories of information will be collected and the policies and procedures that will apply if it is. PIMs should be alert to the need to ensure the public interest in special categories of information is addressed and, where necessary, submissions are made about the weight that should be given to those interests in the circumstances.

599 AGD, *Submission 20*, 17. Government has agreed to expand the Public Interest Advocate regime to warrant-related provisions of the *Crimes Act*, *SD Act*, *TIA Act*, and *ASIO Act* for applications that relate to journalists or media organisations and are for investigations of unauthorised disclosure of government information or a Commonwealth secrecy offence: Australian Government, *Australian Government Response to the Parliamentary Joint Committee on Intelligence and Security Report: Inquiry into the Impact of the Exercise of Law Enforcement and Intelligence Powers on the Freedom of the Press* (Government Response, October 2020) 2–3.

600 National Indigenous Australians Agency (Cth), *Framework for Governance of Indigenous Data* (Framework, 30 May 2024) 7–8.

11.77 For this reason, the need to consider the public interest in special categories of information should be expressed as *including* LPP and the protection of journalists' sources rather than being limited to those. If the recommended amendments are made then accompanying explanatory materials could identify other examples. If they consider it appropriate to do so, PIMs or issuing authorities (through the principal issuing authority) may wish to give further written guidance on what they expect to see in applications including about how the risk of collection of sensitive material has been assessed and special measures (or conditions) to be applied (see Chapters 8, 12).

Recommendation 12: In assessing necessity and proportionality, the list of matters to be considered should include the

...

(e) likelihood that special categories of information, *including* information subject to LPP and information about journalists' sources being collected and, if it is, how the information will be protected;

...

Less intrusive alternatives

11.78 As set out above, *SLAID Act* warrants will infringe on privacy and may in some cases also interfere with property rights and the public interest in protecting special categories of information. How much they do so will depend on the scope of the warrant that is sought and issued, including the nature of the authorised activities. There may be other, less invasive, means available for achieving the goal of investigating or disrupting the relevant serious crimes. This should also form part of the issuing authority's consideration of necessity and proportionality when determining whether to issue a *SLAID Act* warrant.

11.79 Currently, the issuing authority for ATWs must 'have regard to the existence of any alternative means of obtaining the evidence sought to be obtained.'[601] Although not explicitly stated, it seems to be implied that regard should be had to the availability of *less intrusive* means. This is perhaps stated more clearly for NAWs, where the issuing authority must have regard to 'the existence of any alternative, less intrusive, means of obtaining the information sought to be obtained.'[602]

11.80 The Human Rights Law Centre suggested the issuing criteria and relevant considerations should require 'consideration why other alternatives are not appropriate in the circumstances,' although this need not be so strict as to require that agencies actually 'try and fail at all of the other warrants' before being able to 'open the gate to the use of [*SLAID Act*] warrants.'[603] The Law Council drew

601 *Crimes Act* s 3ZZUP(2)(b).
602 *SD Act* s 27KM(2)(e).
603 Anneliese Cooper, HRLC, *Public hearing transcript*, 19 February 2025, 82.

comparison to group warrants in the United Kingdom to suggest NAWs as a group warrant be available as a 'last resort' where it is not reasonably practicable to name or describe those to be targeted by a warrant.[604]

11.81 While not a strict test of 'last resort,' the current requirement for an issuing authority to have regard to the existence of alternative less intrusive means, in combination with the requirement the issuing authority be satisfied of an overarching threshold of necessity and proportionality, is sufficient to ensure that the issuing authority for NAWs will adequately consider the availability of other powers. The requirement for an issuing authority to have regard to alternative measures when deciding an application for an ATW should be strengthened to make particular reference to consideration of *less intrusive* means. For DDWs a 'last resort' test is proposed (see Recommendation 13 below).

Recommendation 12: In assessing necessity and proportionality, the list of matters to be considered should include the:

...

(f) existence of any alternative, less intrusive, means of obtaining the information.

Recommendation on simplified criteria

11.82 As discussed earlier in this chapter, the current list of matters to be considered in determining a warrant application is long. It contains some overlapping provisions and some significant gaps. This review of *SLAID Act* warrants is comprehensive, and comments on individual elements should not be taken in isolation. The introduction of significant new safeguards in the form of retired judges as issuing authorities, PIMs, access to independent technical advice and a statutory duty of candour creates the opportunity for streamlining the considerations relevant to issuing each *SLAID Act* warrant. In addition to maintaining the requirement that the issuing authority be satisfied that there is a reasonable basis for the relevant suspicion founding the application the main issuing criterion should be that the warrant is necessary and proportionate in all the circumstances. To guide the issuing authority, a non-exhaustive list of 6 broad considerations should be included in the legislation for all *SLAID Act* warrants.

604 Law Council, *Submission 23*, 23 [71] referring to Home Office (United Kingdom), *Interception of Communications: Code of Practice* (December 2022) 23 [5.13]–[5.14].

Recommendation 12: Issuing criteria should require that the issuing authority is satisfied that the warrant is necessary and proportionate in all the circumstances. In assessing necessity and proportionality, the list of matters to be considered should include the:

(a) nature and gravity of the offences being investigated (or disrupted);

(b) likelihood that the proposed activity will succeed, as well as the likely value of the resulting intelligence, evidence or disruption;

(c) extent to which the privacy of any person is likely to be interfered with;

(d) extent to which property rights are likely to be interfered with, including through introduction of vulnerabilities;

(e) likelihood of special categories of information, *including* information subject to LPP and information about journalists' sources being collected and, if it is, how the information will be protected; and

(f) existence of any alternative, less intrusive means of obtaining the information.

11.83 These criteria should apply to all *SLAID Act* warrants. One additional criteria should apply to DDWs.

Data disruption warrants should be a last resort

11.84 When determining whether to issue a DDW, the issuing authority is required to have regard to the 'existence of any alternative means of frustrating the commission of the offences …' for which the DDW has been sought.[605] Additionally, a senior AFP or ACIC officer must endorse that a DDW application is 'appropriate in all the circumstances.'[606] However, there is no requirement for the issuing authority to be satisfied that alternative methods would not be feasible or effective.

11.85 This may be contrasted with other unusual powers that are subject to specific thresholds regarding the availability of alternative mechanisms to the power in question. For example, a warrant under the *TIA Act* authorising the interception of communications of a third party who is communicating with a person of interest (a B-party warrant) can only be issued if the issuing authority is satisfied that there are no other practicable methods of identifying the telecommunications services of the person involved in the offences; or it would not otherwise be possible to intercept communications from that person's telecommunications services.[607]

605 *SD Act* s 27KC(2)(c).
606 *SD Act* ss 27KBA(2) (AFP), 27KBB(2) (ACIC).
607 *TIA Act* ss 9(3) (Issued by Attorney-General), 46(3) (Issued by Judge or ART).

11.86 As discussed in Chapter 2, DDWs are not surveillance warrants and should be regarded as a truly extraordinary power. Unlike ATWs and NAWs, which gather information to further investigative processes, DDWs have the direct objective of disrupting data and may cause at least some permanent damage or loss.[608] They should be used sparingly and only in situations where there are no other effective mechanisms, such as arrest and prosecution, available to disrupt serious crimes. The way that AFP described its use of DDWs is consistent with this approach – DDWs have been used in a targeted way where 'traditional investigative actions are not feasible.'[609] AFP gave the example of where 'the volume of victims and effected computers has meant that it is not feasible to apply other methods to prevent continued offending.'[610] AFP's current approach should be encoded in the legislation and not left to good practice alone.

11.87 The Joint Academic Submission proposed that:

> Rather than the decision maker considering the availability of less restrictive means, amending the criterion for the issuance of a warrant so that SLAID warrants may only be issued where the issuing authority is satisfied that no alternative, less-intrusive, means exists by which the warrants' aims might reasonably be achieved.[611]

11.88 I agree in principle with the introduction of this as an additional criterion the issuing authority must be positively *satisfied of* (as opposed to *have regard to*) for DDWs. I also agree in principle with AGD that DDWs should be used only where there are reasons to think other powers 'would be ineffective or likely to be ineffective' but that this should not require the applicant to *have tried* and exhausted all other options before applying for a DDW.[612]

11.89 A 'last resort' threshold for DDWs recognises that they are not a surveillance warrant and are an extraordinary power which should only be used when other options would be ineffective or would probably be ineffective. This threshold should be implemented as a criterion that the issuing authority must be satisfied of (as opposed to 'have regard to') but should not require the applicant to *have tried* and exhausted all other options before applying for a DDW.

Recommendation 13: DDWs should only be available when other measures would not be effective.

608 *SD Act* s 27KE(7), (12)(a).
609 AFP, *Submission 18*, 5 [25].
610 AFP, *Submission 18*, 5 [27].
611 Joint Academic Submission, *Submission 15*, 5 Recommendation 1C.
612 Sarah Chidgey, Deputy Secretary, AGD, *Public hearing transcript*, 20 February 2025, 78.

Chapter 12: Use, disclosure and retention

12.1 AFP and ACIC need appropriate use, disclosure and retention provisions to ensure information collected under *SLAID Act* powers can be used effectively for the law enforcement and criminal intelligence purposes for which Parliament has conferred these powers. At the same time, overly broad use, disclosure and retention is inconsistent with strict control of extraordinary covert powers.

12.2 Currently, statutory safeguards are primarily focused on authorising collection and criminalising unauthorised disclosure. Of course, safeguards on collection are needed and are the focus of most of this report. But modern warrants, especially NAWs, potentially authorise the collection of a lot of data. A large amount of collection is often justified because complex analysis is needed in order to find relevant information in a complex digital environment. Once data has been collected, protections are needed to ensure it is filtered and information not relevant to the warrant purpose is quarantined or deleted to avoid unnecessary or disproportionate intrusions on rights or improper retention of sensitive categories of data. The current requirement to review data at least every 5 years should remain, however, it should be augmented by policy or binding guidelines in some areas.

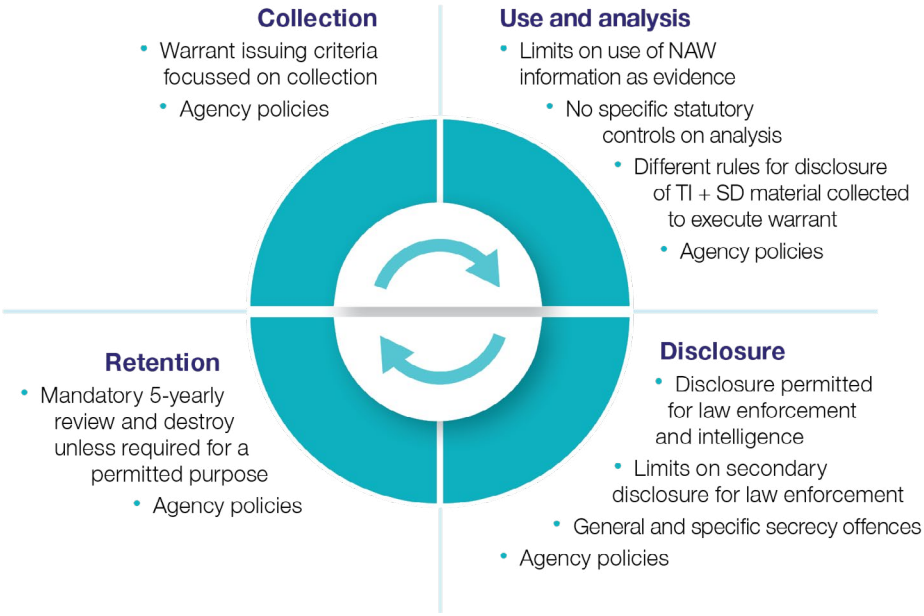
12.3 The currently secrecy provisions that apply to *SLAID Act* warrants are unacceptably complex. Unauthorised disclosure of information collected under *SLAID Act* warrants should continue to be an offence – but the general secrecy provisions in the *Criminal Code* are largely sufficient for this purpose. Reform of the *SLAID Act* provisions is needed, including to ensure they contain a clear list of when *SLAID Act* information can and cannot be disclosed by an official in the course of their duties. Most of the current limitations should stay, including those that strictly limit the use of information obtained under NAWs but some new exceptions are needed including to enable access to legal advice and to ensure any exculpatory material can be disclosed in a prosecution.

Legislative and policy framework

12.4 The framework governing the use, retention and disclosure of information collected under *SLAID Act* powers is complex. It rests on several pieces of general legislation, as well as *SLAID*-specific legislation and both general and SLAID-specific policies. Table 1 provides an overview of the key aspects of legal and policy frameworks that apply to the collection, use, disclosure and retention of such information.[613]

[613] Figure 5 only captures key sources of rules, and omits sources that have limited significance as safeguards such as the *Privacy Act 1988* (Cth) (*Privacy Act*) and *Archives Act 1983* (Cth).

Figure 5 – Key aspects of legal and policy frameworks that apply to lifecycle of data



12.5 Figure 5 illustrates how key aspects of legal and policy frameworks applied to *SLAID Act* information vary across the life cycle of the data, involve overlapping general and *SLAID Act*-specific provisions and policies, and can differ depending on who information is passed to. Although some complexity is to be expected when seeking to regulate the life cycle of information collected under covert powers, the patchwork in place for *SLAID Act* information leads to some areas of concern. It results in both uncertainty where provisions overlap or are unclear and gaps where standard overarching privacy frameworks would (or should) apply in other contexts.

12.6 In many contexts, the Australian Privacy Principles (APPs) contained in the *Privacy Act 1988* (Cth) (*Privacy Act*) provide overarching requirements on the way APP entities (including government agencies) collect, use, disclose and store personal information.[614]

12.7 The *Privacy Act* has limited application to information relating to, or gathered by, the exercise of *SLAID Act* powers:

614 See definition of 'personal information' in the *Privacy Act* s 6; for APPs: s 14 and sch 1.

- The *Privacy Act* does not apply to any acts or practices of ACIC.[615]
- AFP is subject to APPs contained in the *Privacy Act*; however, there are wide exceptions governing use and disclosure for 'enforcement related activities,' including the prevention, detection, investigation of criminal offences, and conduct of surveillance and intelligence gathering activities.[616]

Further exceptions apply where any entity:

- has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in
- reasonably believes that the collection, use or disclosure is necessary in order for the entity to take appropriate action in relation to the matter.[617]

12.8 The fact that the general scheme in the *Privacy Act* itself places little or no limits on the use, retention and disclosure of personal information in the specialised law enforcement and criminal intelligence context of *SLAID* Act powers is not necessarily problematic, provided other safeguards are adequate. Part 3 and Chapter 11 have proposed new safeguards for the collection of information using SLAID Act power. This chapter considers the need for additional safeguards *after* information has been collected.

12.9 The Human Rights Law Centre said that, given the limited application of APPs, 'clearer, more transparent overarching information handling practices, potentially mirroring those under the *Privacy Act'* should be implemented to guide the handling of all information collected under the *SLAID Act*.[618] As Digital Rights Watch pointed out, because *SLAID Act* powers allow information to be collected and shared covertly, 'individuals have no way of knowing that their personal information has been collected and have no way of challenging the lawfulness of the collection, or subsequent uses/disclosures.'[619] This makes it particularly important that the legislative scheme has enhanced safeguards.

615 *Privacy Act* ss 7(1)(a)(iv), 7(1)(h), 7(2)(c). The government has accepted Recommendation 189 of the *2019 Comprehensive Review* that ACIC should be required by legislation to have legally binding privacy guidelines or rules: Government Response to the *2019 Comprehensive Review*, 48.

616 *Privacy Act* s 6 (definitions of 'enforcement body', 'enforcement related activity'). See, for example, *Privacy Act* sch 1 paras 6.2(e) (APP 6 – use or disclosure of personal information) and 8.2(f) (APP 8 – cross-border disclosure of personal information). These exceptions also have an impact on the effect of APP 11: *Privacy Act* sch 1 para 11.2.

617 *Privacy Act* s 16A.

618 HRLC, *Submission 5*, 10 [4.3]; see also Law Council, *Submission 23*, 17–18 [42], 56–57 [215].

619 Digital Rights Watch, *Submission 22*, 4–5.

Criminal offences restricting use and disclosure

12.10 The *SLAID Act* introduced specific criminal offences to the *SD Act* and *Crimes Act* relating to the *use* and *disclosure* of information under a DDW, NAW or ATW.[620] They apply to information about a *SLAID Act* warrant application (including the existence of a warrant), as well as information obtained under those warrants.

12.11 These provisions are remarkably complex. They run to over 24 pages of legislation. Broadly speaking, the framework makes it an offence to disclose the relevant protected category of information, other than where allowed under a detailed list of exceptions. The scope of the exceptions vary between different subsets of information based on the manner in which it was collected, the purpose and context of use/disclosure, and the person/body to whom the information is being disclosed.

12.12 The *SLAID Act* specific offences apply in addition to the more general secrecy offences contained in pt 5.6 of the *Criminal Code* and the secrecy offences contained in the enabling legislation for AFP and ACIC.[621]

> The combination the specific *SLAID Act* secrecy offences and general secrecy offences results in a legislative regime that is extremely complex.

Unnecessary complexity in secrecy provisions

12.13 Complexity is a barrier to public understanding of how information about *SLAID Act* warrants, and the information obtained under them, can be used. Excessive complexity can also make it difficult for law enforcement agencies to use the powers effectively and may lead to an increased risk of inadvertent noncompliance and unintended limits on disclosure. As noted by the Human Rights Law Centre, this complexity has resulted in 'unnecessary uncertainty in an area that requires more, rather than less, clarity and precision.'[622]

12.14 The framing of the specific offences introduced by the *SLAID Act* results in disclosure rules that are in some instances too restrictive. For example, AFP and ACIC were constrained from voluntarily providing this review with even general information about their use of *SLAID Act* warrants. Despite the agencies' willingness to cooperate with this review, every time I sought documents or a meeting about

620 Relevant provisions include *Crimes Act* ss 3ZZUK, 3ZZVH; *SD Act* ss 44, 44A, 45; *TIA Act* ss 5, 63AD, 63AE, 108(2)(cd).

621 Broadly speaking, AFP and ACIC officials must not make a record of, or communicate, information that is acquired in the course of their duties other than where allowed under a list of exceptions including the performance or exercise of their duties: *Australian Federal Police Act 1979* (Cth) s 60A (*AFP Act*); *ACC Act* s 51.

622 HRLC, *Submission 5*, 10 [4.3].

the *SLAID Act* powers it was necessary for me to exercise my statutory power to issue a notice requiring that information be given to my office.[623] This added delay and complexity, without adding any value. Similarly, as discussed in Chapter 4, AFP and ACIC feel constrained from providing public statements about the use and effectiveness of *SLAID Act* powers; changing this would provide the opportunity for more transparency. Most concerning is the perhaps inadvertent limit on providing potentially exculpatory material in a criminal prosecution. This limit, and the need for urgent amendments, is discussed later in this chapter. Similarly, a person cannot currently obtain legal advice about an assistance order directed at them for DDWs and NAWs. This is a problem and also requires rectification as soon as possible.

12.15 The current provisions also unnecessarily blur 'use' and 'disclosure' in some instances. For example, it is a crime to use NAW information in evidence in most prosecutions. While NAW information should not be able to be used for a prosecution, this can be achieved simply by having a rule that makes it inadmissible as Crown evidence. It is not necessary to make it a crime as well.[624]

12.16 At the same time, the exceptions to the specific offences can in some instances enable the disclosure of a broad range of information with few limits. This is particularly the case where information is given to ASIO, ASD, Australian Secret Intelligence Service or Australian Geospatial-Intelligence Organisation because it 'relates or appears to relate to any matter within' the very broad functions of those agencies.[625] Further, where protected information is disclosed because it relates to those agencies' functions, exceptions to the specific offence also apply to all use, recording and communication of that information by an agency head / employee / affiliate / staff member of those agencies in the performance of their functions.[626]

12.17 AGD said, 'the main reason for the complexity of the use and disclosure framework results from differences between the warrant types.'[627] However, the department did acknowledge that there are 'opportunities to simplify and consolidate the secrecy, use and disclosure provisions that relate to the *SLAID Act* powers' and that 'this is a key area of focus for the electronic surveillance reform process.'[628]

623 *INSLM Act* s 26.

624 *SD Act* s 45B(1), (3), (10).

625 *SD Act* ss 45(4)(c)-(d), 45B(4)(d)-(e).

626 The disclosure rules in the *ASIO Act* and *IS Act* would apply but these are permissive and allow the agencies to disclose a broad range of information to Australian and foreign agencies for intelligence and security purposes as well as, in some instances, law enforcement: *ASIO Act* s 18(2), s 18(3), s 18(4A), s 19 and s 19A. While ASIS, AGO and ASD are not responsible for law enforcement functions, they are not prevented from communicating any intelligence that is relevant to serious crime to the appropriate law enforcement authorities*: IS Act* s 11(2), subject to certain rules regarding privacy: s 15(1A); unauthorised communication is an offence: s 39.

627 AGD, *Submission 20*, 21.

628 AGD, *Supplementary response 28*, 7 in line with the *2019 Comprehensive Review* finding that the secrecy offences are 'overly-prescriptive, complex and in some cases inconsistent': *2019 Comprehensive Review* vol 2, 398 [30.48] (Recommendation 120). See also AGD, *Submission 20*, 21.

Greater reliance on general secrecy offences

12.18 Part 5.6 of the *Criminal Code* contains broad secrecy offences that apply to 'Commonwealth officers' (including contractors) as well as a narrower offence that applies to non-officials.[629] The government recently endorsed the policy that specific secrecy offences should only be resorted to where criminal liability differs in significant and justifiable ways from general secrecy offences.[630] Part 5.6 was recently subject to an INSLM review: *Secrecy Offences – Review of Part 5.6 of the Criminal Code 1995* (2024 INSLM Secrecy Review). The following discussion also takes account of that review and the government response.

Commonwealth officials

12.19 For Commonwealth officials it is currently a serious deemed harm offence under s 122.1 of the *Criminal Code* to 'deal with' or disclose 'information relating to operations, capabilities or technologies of, or methods or sources used by, a domestic or foreign law enforcement agency.' I recently recommended that this be amended to 'information that relates to the technologies, capabilities and methods used to exercise special electronic surveillance powers.' The government agreed 'in principle' to this recommendation.[631] Either way, this 7-year (10-year if aggravated) offence clearly covers and will continue to cover information about the technologies, capabilities and methods used to exercise *SLAID Act* powers.

12.20 It is also currently a 7-year (10-year if aggravated) offence under s 122.2 of the *Criminal Code* to disclose any information that 'interferes with or prejudices the prevention, detection, investigation, prosecution or punishment of a criminal offence against a law of the Commonwealth' or is likely to do so. I recommended that this be retained but moved to a different offence (s 122.4, a 2-year offence). The government response indicated an intention to retain 'prejudicing the prevention, detection, investigation, prosecution or punishment of a criminal offence against a law of the Commonwealth' in the more serious s 122.2 offence.[632] Either way, any unauthorised disclosure of *SLAID Act* information, including the existence of a particular warrant or information obtained under it, would continue to be covered by the *Criminal Code* offences and, based on the government response, a 7-year (or 10-year if aggravated) offence.

629 *Criminal Code Act 1995* (Cth) s 121.1(1) (definition of 'Commonwealth officer') (*Criminal Code*).
630 AGD, *Review of Secrecy Provisions* (Final Report, 21 November 2023) 8 [18] (AGD Secrecy Provisions Review). See also Attorney-General (Cth), 'Reforms to Commonwealth Secrecy Offences' (Media Release, 21 November 2023).
631 *2024 INSLM Secrecy Review*, 3. Government agreed in principle to this recommendation: Australian Government, *Government Response to the Independent National Security Legislation Monitor Report – Secrecy Offences: Review of Part 5.6 of the Criminal Code Act* 1995 (Government Response, November 2024) 3.
632 *2024 INSLM Secrecy Review*, 5 Recommendation 6.

The *Criminal Code* already makes it a crime for a Commonwealth official to disclose any information relating to *SLAID Act* capabilities or any information that might prejudice law enforcement operations.

12.21 Any disclosure by a Commonwealth official that reveals the technologies, capabilities and methods used to exercise *SLAID Act* powers should be an offence. This type of conduct is and will remain criminalised by pt 5.6 of the *Criminal Code*. Similarly, any disclosure by a Commonwealth official that risks prejudicing the prevention, detection, investigation, prosecution or punishment of a criminal offence against a law of the Commonwealth should be an offence. This type of conduct is and will remain criminalised by pt 5.6 of the *Criminal Code*. In view of this I see no need for additional offences for Commonwealth officials to be retained in the *SLAID Act* specific provisions. Retaining the *SLAID Act* convoluted regime for specific secrecy offences would also be inconsistent with the government's recently endorsed principles to be used in framing secrecy offences and to guide work to reduce the number of these offences.[633]

12.22 However, it is necessary to ensure that Commonwealth officials can only deal with and disclose *SLAID Act* information in limited and appropriate circumstances. A relatively simple way to achieve this would be to rely on the 'course of duties' exception for the *Criminal Code* offences by including in the *SLAID Act* provisions a clear list of when officials can use and disclose *SLAID Act* warrant information.[634] If necessary, a regulation-making power could be added in the *SLAID Act* provision to extend the 'course of duties' if strictly necessary in future. The provision could say that other uses of *SLAID Act* information are not permitted unless expressly authorised under some other law. This would be much simpler than the current *SLAID Act* framing of making everything an offence and having exceptions plus the complexity of the *Criminal Code* and other secrecy offences applying over the top. The *Australian Federal Police Act 1979* (Cth) and *Australian Crime Commission Act 2002* (Cth) also have a similar course of duties exception.[635]

Legislation can set out when it is proper for an official to use or disclose *SLAID Act* information. This will automatically tie in to an existing exception to the *Criminal Code* offences.

633 AGD Secrecy Provisions Review 8 [18]. See also Attorney-General (Cth), 'Reforms to Commonwealth Secrecy Offences' (Media Release, 21 November 2023).
634 *Criminal Code* s 122.5(1)(a).
635 *AFP Act* s 60A(2)(c) and (f); *ACC Act* s 51(2) and (4).

12.23 AGD said that it is appropriate for the use of *SLAID Act* information to be much more restricted than general information that law enforcement agencies may collect, noting the need for:

- 'stricter limits' on when such information can be used, disclosed or given in evidence
- 'closely controlling secondary uses and disclosures by agencies and third parties that may receive such information, including state or territory agencies, and industry partners'
- imposing stricter controls on when unlawfully obtained information may be used, disclosed and given in evidence.[636]

I agree. The proposed 'course of duties list' and rules on admissibility should reflect this.

12.24 I note that the *Criminal Code* has a carefully crafted set of defences, including for officials. These include communication to an integrity agency or a court or for the purpose of obtaining legal advice.[637] I consider this to be another attraction of reliance on the *Criminal Code*. It brings greater consistency to criminal law policy and will reduce the need to replicate exceptions.

Non-officials

12.25 There is a case for it to continue to be an offence for a non-official to disclose information about *SLAID Act* capabilities or other information that would prejudice a law enforcement operation. Non-officials include contractors who may be assisting to execute a warrant, those who have been served with an assistance order and journalists and others who have received the information.

12.26 Contracted service providers and their employees who are assisting with the execution of a warrant or development of the capabilities needed to execute *SLAID Act* warrants are already deemed to be 'Commonwealth officers' and so are covered by the offences above.[638] These are 7-year offences (10-year if aggravated). No doubt there are also non-disclosure clauses in those contracts. If an 'industry partner' is privy to information about the execution of a *SLAID Act* warrant or the information under it in a capacity other than under a contract then the general offence in s 122.4A (a 5-year offence) for a disclosure that would 'interfere with or prejudice the prevention, detection, investigation, prosecution or punishment of a criminal offence against a law of the Commonwealth' would still apply. It is difficult to see the need for any other offences beyond these for contractors and 'industry partners.'[639]

636 AGD, *Supplementary submission 28*, 7.
637 *Criminal Code* 122.5; *2024 INSLM Secrecy Review*, ch 9.
638 *Criminal Code*, s 121.1 (definition of 'Commonwealth officer' (f) and (g)).
639 If they are required to provide assistance under a statutory scheme such as *TOLA Act*, other offences apply to unauthorised disclosures: see, for example, *Telecommunications Act 1997* (Cth) s 317ZF. In addition, there are offences that apply to other schemes, see, for example, offences prohibiting unauthorised dealing in intercepted information or interception warrant information: *TIA Act* s 105.

12.27 My 2024 Secrecy Review report has a lengthy discussion about the reasons why offences for journalists and other non-officials should be harm-based. For the reasons given in that report, general offences for non-officials, including journalists, should be strictly harm-based and relate only to disclosures (not, for example, receipt). The government accepted the relevant recommendations, although it said the bar for disclosures about law enforcement information should remain at '*interfere with or prejudice* the prevention, detection, investigation, prosecution or punishment of a criminal offence against a law of the Commonwealth.'[640]

12.28 There is a risk that a person who has been served with an assistance order may disclose the existence of a warrant to a subject of the warrant or their criminal associates and thus prejudice the investigation. This would seem to be adequately covered by the existing 5-year offence in s 122.4A of the *Criminal Code* for a disclosure that would 'interfere with or prejudice the prevention, detection, investigation, prosecution or punishment of a criminal offence against a law of the Commonwealth,' and this offence could be highlighted in the paperwork used to notify a person of an assistance order. While it is true that omitting to do an act required under an assistance order is currently subject to a higher penalty of imprisonment for 10 years or 600 penalty units, the 5-year penalty for the offence in s 122.4A of the *Criminal Code* seems proportionate for outsiders who are not Commonwealth officials.[641] This review did not receive any submission justifying the necessity for retaining a 7 to 10-year penalty offence for persons who are not Commonwealth officials.

> The *Criminal Code* offences should be relied on for non-officials, including journalists.

12.29 As with the offences for Commonwealth officials, there are carefully considered defences in the *Criminal Code.* Again, I consider this to be another reason why the *Criminal Code*, rather than a multitude of specific offences, should be relied on as far as possible.

State and territory police

12.30 Complete reliance on the *Criminal Code* offences may leave an inconsistency between Commonwealth officials and state and territory police who they cooperate or share information with. It would still be an offence for anyone to disclose information that would interfere with or prejudice the prevention, detection, investigation, prosecution or punishment of a criminal offence against a law of the Commonwealth, but for Commonwealth officials the penalty would be higher (7 or 10 years if aggravated compared to 5 years for other persons including state and territory officials). Commonwealth officials would also be subject to an additional

640 I would have raised the bar to '*seriously impeding* the prevention (etc): *2024 INSLM Secrecy Review,* 189 (Recommendation 12); Australian Government, *Government response to the Independent National Security Legislation Monitor report – Secrecy Offences: Review of Part 5.6 of the Criminal Code Act 1995* (Government response, November 2024) 12.

641 *SD Act* ss 64A(8), 64B(3).

deemed harm offence under s 122.1 which, as discussed above, would cover either 'information relating to operations, capabilities or technologies of, or methods or sources used by, a domestic or foreign law enforcement agency' or 'information that relates to the technologies, capabilities and methods used to exercise special electronic surveillance powers.'

12.31 Presumably, state and territory officials would also be covered by state and territory offences concerned with discourse that may prejudice investigation (etc.) of a state or territory offence.

12.32 If, after relevant consultation including with states and territories, it is considered necessary to have a specific Commonwealth offence beyond the offence in s 122.1 for state and territory officials who disclose information about or obtained under *SLAID Act* warrants then a relatively simple option would seem to be to deem them to be Commonwealth officials for this specific category of information. This could then be linked to the *Criminal Code* offences to ensure they apply equally.

Recommendation 14: The secrecy provisions should be reformed in accordance with the following principles:

(a) Removal of unnecessary complexity and inconsistency.

(b) Reliance on the general secrecy offences in the *Criminal Code*.

(c) Retention of strict limits on the way officials can use SLAID Act information, potentially through positively defining what use is permitted in the 'course of duties.'

...

Ability to obtain legal advice on an assistance order

12.33 One area that requires specific and prompt reform is the current limitation under which a person who is subject to an assistance order cannot disclose information to a lawyer in good faith in order to seek advice on the assistance order.

12.34 As discussed in Chapter 14, an assistance order requires a person to provide 'any information or assistance that is reasonable and necessary' for a law enforcement officer to disrupt data that is the subject of a DDW, access data in a computer subject to a NAW or take over an online account subject to an ATW. Failure to comply is a serious offence.[642] What sort of assistance is 'reasonable' and whether the person has to comply are the kinds of things an individual may well want to seek legal advice on.

642 *Crimes Act* s 3ZZVG(3); *SD Act* ss 64A(8), 64B(3).

12.35 As Dr Walker-Munro observed, disclosure of the existence of an assistance order necessarily reveals the existence of the *SLAID Act* warrant or emergency authorisation for which the order was sought and issued.[643] It is currently an offence for any person to make this type of disclosure, including if they want to seek legal advice on an assistance order associated with a DDW or NAW.[644]

12.36 This limitation on seeking legal advice does not arise for ATWs because the *Crimes Act* expressly excepts use or disclosure of information for the purposes of obtaining legal advice in relation to pt IAAC (which includes the provisions for ATW assistance orders).[645] The Revised Explanatory Memorandum notes this exception is included because '[l]egal advice may need to be sought on the interpretation of the account takeover warrant provisions to ensure that AFP and ACIC are acting in accordance with the law when exercising this power.'[646]

12.37 I agree with the Law Council's position that 'an individual in receipt of an assistance order should not be precluded from obtaining legal advice in light of the potentially serious repercussions of complying with that order.'[647] A person should not be prevented from seeking legal advice to understand their obligations under such an order or to understand the other legal effects of that order (for example, concerning the protection from civil liability for things done in compliance with the order).

12.38 It appears that AGD's policy position aligns with this view. However, the department suggested that the exception for 'use and disclosure of information in connection with the administration or execution of the Act … would generally include seeking legal advice in connection with an order served on a person.'[648] I find this an ambitious interpretation of the words in the Act. Further, the Revised Explanatory Memorandum does not indicate this provision was intended to extend to nonofficials seeking legal advice. Instead, it explains that:

> [The 'administration or execution' exception was introduced so that] the Department and the Minister responsible for administering and executing the *SD Act* can receive and share information for administrative purposes. For example, information regarding how each warrant has been used can be provided to the Minister outside of the preparation of the annual reports.[649]

12.39 Even before seeking legal advice about the assistance order itself, a person would be in the impossible position of not being able to seek legal advice on whether the administration exception to the secrecy offence applied to seeking legal advice

643 Brendan Walker-Munro, *Submission 3,* 12.
644 *Crimes Act* ss 3ZZUK (definition of 'protected information'), 3ZZVH; *SD Act* ss 44(1)(b)(i), 44A(c), 45, 45B.
645 *Crimes Act* s 3ZZVH(3)(g).
646 Revised Explanatory Memorandum 199 [1174].
647 Law Council, *Supplementary response 26*, 1. An assistance order exposes a person to liability for a serious criminal offence carrying the high penalty of 10 years imprisonment and/or 600 penalty units.
648 AGD, *Supplementary submission 28* 8; *SD Act* ss 45(4)(aa), 45B(4)(a).
649 Revised Explanatory Memorandum 213 [1271].

about the order they are subject to without risking committing a secrecy offence.[650]

12.40 If, as recommended above, the *SLAID Act* offences for non-officials are repealed and reliance is instead placed on the general *Criminal Code* offences then the defence in s 122.5(5A) of the *Criminal Code* will allow a person to disclose information in order to seek legal advice about an offence against that part of the *Criminal Code*. This may not be broad enough to enable a person to disclose information in order to seek advice on an assistance order made under another Act.

12.41 Necessary amendments should be made to clearly permit a person to seek legal advice about an assistance order they may be required to comply with.

Recommendation 14: The secrecy offences should be reformed in accordance with the following principles:

...

(d) There should be no barrier to a person seeking legal advice about an assistance order they may be required to comply with.

...

Specific limitations on use and disclosure of NAW information

12.42 Information obtained under a NAW is subject to more restrictions on use and disclosure than information obtained under ATWs and DDWs. This is consistent with NAWs being an intelligence warrant and having a much lower threshold and wider scope than other criminal law related warrants.

12.43 The main restriction is that, in general, protected NAW information may not be admitted in evidence in criminal proceedings.[651]

12.44 I consider that it remains appropriate to retain strict limits on the use of NAW information, including as evidence in criminal proceedings. However, 2 changes are needed: exculpatory material must be able to be disclosed to (and used by) a defendant; and NAW information should not be able to be used in proceeds of crime proceedings.

650 This is similar to the issues relating to the legal advice defence for secrecy offences in pt 5.6 of the *Criminal Code*: see *2024 INSLM Secrecy Review*, 217–18 [9.98]–[9.101].

651 *SD Act* s 45B(3). An exception exists for criminal proceedings relating to a breach of the secrecy provisions in the *SD Act* (s 45B(10)); see also s 45B(4), (5) and (7).

Prosecution duty to disclose

12.45 The current strict secrecy provisions and prohibition on use of NAW information in evidence may risk the prosecution being unable to fulfil their duty of disclosure – for example, where potentially exculpatory material is not disclosed to the defendant. This runs counter to the obligation to provide a fair trial.[652] The Commonwealth Director of Public Prosecutions describes the duty of disclosure as a 'significant aspect of the administration of criminal justice and the court's capacity to ensure the accused's right to a fair trial'. Failure to disclose may result in a miscarriage of justice.

12.46 The scope of the duty includes material that can be seen 'on a sensible appraisal' to run counter to the prosecution case; might be reasonably expected to assist the accused to advance a defence; or might reasonably be expected to undermine the credibility of a material prosecution witness.[653]

12.47 An amendment is needed to ensure that all material that would ordinarily need to be disclosed to and by the prosecution can be disclosed, even if it was obtained under a NAW. If the defence wishes, it should be able to use that material subject to any court orders that have been made about the way sensitive information is to be managed in the proceeding.

Recommendation 14: The secrecy offences should be reformed in accordance with the following principles:

...

(e) Potentially exculpatory material obtained under a network activity warrant should be able to be disclosed in accordance with the usual prosecutorial duty of disclosure.

...

652 Law Council, *Submission 23*, 17 [38].

653 CDPP, *Statement on Disclosure: Statement on Disclosure in Prosecutions Conducted by the Commonwealth* (Policy, March 2017) 3 [2]; 3 [3].

Use of network activity warrant information in proceeds of crime proceedings

12.48 There are certain exceptions to the limitation on the use of NAW information in proceedings, including that protected NAW information may be admitted in evidence in 'a proceeding that is not a criminal proceeding.'[654] This was intended to allow protected NAW information to be admitted in evidence in proceedings questioning the validity of a warrant.[655]

12.49 However, there is some ambiguity about whether the exception also enables protected NAW information to be admitted in proceedings under the *Proceeds of Crime Act 2002* (Cth) (*POCA Act*), which are civil rather than criminal proceedings.[656] AFP has not used protected NAW information in these proceedings.[657]

12.50 In the public hearing and in a subsequent supplementary written submission, AGD indicated that s 45B of the *SD Act* was *not* intended to allow protected NAW information to be used in *POCA Act* proceedings.[658] It further noted that:

> While paragraph 45B(1)(b) would appear to permit admission of protected network activity information in proceeds of crime proceedings, in practice, other aspects of section 45B would likely preclude that approach. In particular, subsections 45B(4) and (5) would not provide a basis for such information to be disclosed to, or used by, persons undertaking an unexplained wealth investigation for investigative purposes.[659]

12.51 The policy intent that s 45B(10)(b) apply only to certain civil proceedings is not clearly reflected in the statutory text. It is also not clear that other aspects of s 45B would preclude the use of protected NAW information as evidence in *POCA Act* proceedings. Protected NAW information, other than information that was obtained from the use of a surveillance device under a NAW, may be used, recorded, communicated or published, or admitted into evidence if it is necessary to do so in order for AFP to collect, correlate, analyse or disseminate criminal intelligence in the performance of its functions.[660] Relevantly, those functions include functions under the *POCA Act*.[661]

12.52 To avoid any uncertainty, I consider that the *SD Act* should be amended to make clear that protected network activity information cannot be admitted in evidence in *POCA Act* proceedings.

654 *SD Act* s 45B(10)(b).
655 AGD, *Supplementary submission 28*, 4; Revised Explanatory Memorandum 117 [608].
656 *Proceeds of Crime Act 2002* (Cth) s 315.
657 AGD, *Supplementary submission 28*, 4.
658 AGD, *Supplementary submission 28*, 4.
659 AGD, *Supplementary submission 28*, 4.
660 *SD Act* s 45B(5)(a), read alongside *AFP Act* s 8.
661 *AFP Act s* 8(1)(bd).

Recommendation 14: The secrecy offences should be reformed in accordance with the following principles:

...

(f) The law should be clarified to put beyond doubt that network activity warrant information cannot be admitted in evidence in proceedings under the *Proceeds of Crime Act 2002* (Cth).

ACIC proposal on increased use and sharing of TI and SD information

12.53 The main thing authorised by a NAW is access to data held on computers. A NAW can also authorise intercepting telecommunications or using a surveillance device, but only for the purposes of executing the NAW (i.e. only to facilitate getting information from a computer).[662] Reflecting this restricted use, information collected under a NAW using interception or surveillance device capabilities can only be used or disclosed for a limited set of purposes.[663]

12.54 One of the purposes that this information can be used for is where necessary to prevent or reduce a risk of serious harm or where the information relates to activities prejudicial to security within the meaning of the *Australian Security Intelligence Organisation Act 1979* (Cth) (*ASIO Act*). This covers a number of 'very serious circumstances,' but it does not cover every situation where evidence of some form of criminality may be incidentally identified through the use of TI or SD powers that are only authorised to enable a NAW to be executed.[664]

TI and SD material can be disclosed in very serious circumstances, but not for every possible offence incidentally identified.

12.55 ACIC suggested that consideration be given to whether these limitations on the use and communication of TI and SD material could be relaxed. ACIC specifically referred to 'not being able to use the information to apply for other warrants, including other NAWs.'[665] It also provided examples of where it had been unable to use and communicate information relating to the detection, prevention or frustration of a serious criminal offence because that information had been identified

662 *SD Act* ss 27KP(2)(h), (i). A separate interception warrant or surveillance devices warrant is required if ACIC or AFP wish to undertake interception or use a surveillance warrant for other purposes: ACIC, *Submission 17*, 7.

663 *TIA Act* s 63AE (permitted uses of NAW intercept information); *SD Act* s 45B(4) (permitted uses of protected NAW information).

664 *SD Act* ss 45B(4)(c)-(d); *TIA Act* s 63AE(2).

665 ACIC, *Submission 17*, 7–8.

incidentally when utilising interception or surveillance device capabilities to enable execution of a NAW.[666]

12.56 There was some uncertainty from ACIC's evidence in the public hearing about the extent of their collection of TI and SD information to execute computer access under a NAW. Evidence subsequently provided in a private hearing indicated that this collection may be quite extensive in some situations, which they consider are necessary for assisting covert execution of the warrant at the right time and in relation to the right computer(s).[667]

12.57 When the *SLAID Act* was introduced, a distinction was drawn between information obtained under a NAW using computer access capabilities and other capabilities. For example, for information obtained by using a surveillance device under a NAW, the Revised Explanatory Memorandum noted, '[t]he purpose of this power is to facilitate the execution of the warrant, not to collect intelligence.'[668] Similar limitations apply to information obtained using telecommunications interception under a DDW and computer access warrants.[669]

12.58 AGD supported the retention of this distinction and observed that it reflected the different purposes and relevant thresholds of a NAW compared with an interception warrant or surveillance device warrant:

> noting particularly that the thresholds for a network activity warrant are lower … than for an interception warrant, we would have a concern then about an ability to use information that would in other circumstances be subject to a higher threshold, and having this as a sort of exception with a lower threshold access to that information that's ultimately for use.
>
> So with the framework as it is currently is, I think that that would be an issue to open the way to use the information.[670]

12.59 Interception and surveillance device warrant thresholds and how they interact is something that extends beyond the *SLAID Act* warrants. I understand this is being considered in the context of broader ESR. However, I agree with AGD that '… at the moment there would be an issue in allowing further use and disclosure of information that wasn't originally obtained under the thresholds that were applicable to that information.'[671]

It is not appropriate at this time to relax restrictions on use and disclosure of information incidentally collected under a NAW.

666 Wendy Darling, ACIC, *Public hearing transcript*, 20 February 2025, 55–6.
667 INSLM, *Summary of private hearing – ACIC*, 11 March 2025, 3-4.
668 Revised Explanatory Memorandum 116 [603].
669 *TIA Act* ss 63AC, 63AD; Revised Explanatory Memorandum 110 [570].
670 Sarah Chidgey, AGD, *Public hearing transcript*, 20 February 2025, 76.
671 Sarah Chidgey, AGD, *Public hearing transcript*, 20 February 2025, 76.

Recommendation on use and disclosure provisions

Recommendation 14: The secrecy offences should be reformed in accordance with the following principles:

(a) Removal of unnecessary complexity and inconsistency.

(b) Reliance on the general secrecy offences in the *Criminal Code*.

(c) Retention of strict limits on the way officials can use information obtained under warrants, potentially through positively defining what use is permitted in the 'course of duties'.

(d) There should be no barrier to a person seeking legal advice about an assistance order they may be required to comply with.

(e) Potentially exculpatory material obtained under a NAW should be able to be disclosed in accordance with the usual prosecutorial duty of disclosure.

(f) The law should be clarified to put beyond doubt that NAW information cannot be admitted in evidence in proceedings under the *Proceeds of Crime Act 2002* (Cth).

Other controls on use, analysis and retention

12.60 Apart from the offences that relate to the disclosure of information and limits on use of NAW material in evidence, there are limited controls that apply to use and analysis of information. There is a statutory requirement to keep data secure and to review it every 5 years and then destroy it if it is 'not likely' to be required in connection with a permitted purpose. Several submissions to this review raised concerns about the sufficiency of these controls, particularly in regard to protection of special categories of data, the use of artificial intelligence and the review and destruction of *SLAID Act* information.[672]

Requirement to review and destroy information

12.61 The requirement to destroy information that it is not necessary to retain is a fundamental safeguard in any surveillance framework and assists in ensuring that limitations imposed on the right to privacy are necessary and proportionate.[673] The Ombudsman stressed that 'regular review for retention or destruction of records created using a covert and intrusive power is critical to the responsible use of the power.'[674]

12.62 Two specific requirements apply to AFP and ACIC concerning the destruction of information obtained under *SLAID Act* warrants. The first is a general requirement to destroy information 'as soon as practicable' if satisfied that the information is not likely to be required for a broad range of permitted purposes. However, like similar tests in other legislation, this general 'if satisfied' requirement does not impose a positive obligation to review information or make a decision. The second requirement does impose a specific obligation to review information obtained under a *SLAID Act* warrant every 5 years and destroy that information unless it has been assessed as being 'likely' to be required for a broad range of permitted purposes.[675]

> AFP and ACIC must review information obtained under a *SLAID Act* warrant every 5 years.

12.63 The situation is more complex for information that has been disclosed to other Australian agencies. However, generally speaking, there is a requirement for Australian law enforcement and intelligence agencies to review and destroy

672 Law Council, *Submission 23*, 51–5; AJF, *Submission 7*, 5. AHRC, *Submission 21*, 12–13; Digital Rights Watch, *Submission 22*, 6–7.

673 *2019 Comprehensive Review* vol 2, 414 [30.120].

674 Ombudsman, *Submission 11*, 7.

675 *Crimes Act* s 3ZZVJ; *SD Act* ss 46(1), 46AA(1). The permitted purposes include use in civil and criminal proceedings as well as a broad range of police, integrity and intelligence matters: see, for example, *SD Act* ss 45(4)–(5), 45A(1); *Crimes Act* s 3ZZVH(3)–(4) (note that the reference in ss 3ZZVJ(b)(i) to 3ZZVH(2) appears to be a drafting error). Both ACIC and AFP have obligations to retain certain material under the *Archives Act 1983* (Cth); however, these requirements do not apply where there are destruction requirements such as those that apply to *SLAID Act* information under the *SD Act* and *Crimes Act*.

information they have received which was collected under a DDW or NAW every 5 years.[676] The *Crimes Act* does not contain an equivalent express obligation for information that was obtained because an ATW was used. While that should be rectified, it is noted that AFP advised that it is rare for information to actually be collected under an ATW, rather the ATW facilitates collection under other authorities (such as a computer access warrant or a controlled operation). This highlights the need for a rule that requires periodic review to be broader than for only *SLAID Act* information. This is matter for the ESR project.

12.64 The Australian Human Rights Commission was concerned that a requirement that warrant information be reviewed every 5 years is insufficient – they believed it should be more frequent.[677] The Human Rights Law Centre and Law Council suggested that the current requirement to review and then destroy information obtained under a warrant every 5 years should be reduced to ever 3 years.[678]

12.65 ACIC said that it 'regularly reviews' all intelligence and information obtained under surveillance powers to ensure 'collected material remains relevant and required for a permitted purpose, notwithstanding the longer review and destruction periods mandated under the legislation.'[679]

12.66 The requirement to destroy information after 5 years when it is not necessary to retain should be seen as an outer limit, intended to apply to every case, but there will be circumstances where more regular review is warranted. Where there is a large volume of information collected – for example, under a broadly framed NAW with a high likelihood of capturing information about persons who are not subject to investigation – more regular review requirements are warranted. In this context, a more regular review period should be stipulated as a matter of binding administrative guidance and/or a warrant condition.

12.67 In addition to the '5 year rule,' AFP (but not ACIC) has a positive duty, under the *Privacy Act*, to take reasonable steps to destroy or de-identify personal information about individuals where that information is no longer required for any purpose for which it may be used or disclosed under the APPs (and provided the information is not a Commonwealth record and retention is not required by a law or court order).[680] However, the breadth of permissible use and disclosure for 'enforcement related activities' means this destruction requirement has limited effect.

12.68 Noting that 5 years have not yet passed since the *SLAID Act* warrants were first introduced, it is difficult to reach a clear view about whether the review and destruction requirements are operating as intended. However, it is noted that the Ombudsman has raised concerns about AFP and ACIC noncompliance with destruction requirements in similar regimes for the exercise of covert and intrusive powers and observed that 'the review and destruction of records created through

676 *SD Act* ss 46(2)(b), 46AA(2)(b).
677 AHRC, *Submission 21*, 12–13 [41] (Recommendation 9).
678 HRLC, *Submission 5*, 10 (Recommendation 6); Law Council, *Submission 23*, 53–5 [200] (Recommendation 27).
679 ACIC, *Submission 17*, 9.
680 *Privacy Act* sch 1 para 11.2.

use of DDWs and ATWs is an area of concern my Office will continue to closely monitor.'[681]

12.69 At this stage I recommend that the '5 year rule' be retained and extended to information that was accessed due to an ATW. Internal agency policies and/or binding administrative guidance should make provision for earlier reviews of particularly sensitive categories of information. Issuing authorities can take into account the adequacy of these polices for sensitive information when they are issuing warrants or attaching conditions to warrants (see discussion of 'special categories of information' in Chapter 11).

Recommendation 15: Information accessed under a *SLAID Act* power should be reviewed at least every 5 years and destroyed if no longer required for identified purposes. Internal agency policies and/or binding administrative guidance should make provision for earlier reviews of particularly sensitive categories of information.

Policies

12.70 While agency policies do not form part of the legislation under review, they can provide practical safeguards, so they help to inform a view on whether there is a need for legislative change. Policy is currently the main safeguard for what happens to information *inside* an agency, at least between the mandatory 5-year review points.

12.71 As part of this review, I reviewed copies of AFP and ACIC policies that relate to the use, retention and disclosure of sensitive categories of information obtained under warrants.[682] The agencies each have general policies that apply to disclosure of information collected during investigations. These contain varying levels of information and guidance on the privacy concerns that are relevant to information gathered by use of *SLAID Act* powers. Beyond its general privacy policy, AFP in particular provided a number of policy documents that relate specifically to handling of special categories of information, including LPP, parliamentary privilege and investigations involving journalists. In relation to LPP, the Law Council submitted that the guidelines for search warrants (made in 2001) are outdated and that there is a need for equivalent guidelines to be developed for electronic material.[683]

12.72 Some of the general policies that are relevant to privacy considerations, such as AFP's Privacy Policy and ACIC's Information Handling Protocol, are made

681 Ombudsman, *Submission 11*, 7.
682 This was done by use of the Monitor's powers under s 24 of the *INSLM Act*.
683 Tim Game SC, *Public hearing transcript*, 19 February 2025, 51. See also Law Council, 'Execution of AFP Search Warrants on Lawyers' Premises' (Web Page, 5 May 2021).

accessible to the public.[684] Others are classified and for internal use only. Submitters to this review noted that the gaps in publicly available information about policies for handling information make privacy arrangements opaque. They said it would beneficial for practices in that regard to be more transparent.[685] AGD said it 'wouldn't have a problem' with greater transparency and public engagement regarding policies and procedures about special categories of information, within the limits of 'what can appropriately be made public.'[686] I agree that there is opportunity to provide further public clarity about information handling practices without revealing information that may compromise operations and investigative techniques.

Gaps in publicly available information about policies for handling information make privacy arrangements opaque.

12.73 Privacy and the handling of special categories of information are not the only areas where internal agency policy controls are currently the main 'safeguard.' Once information has been collected. The Commonwealth position on sharing information where there is a risk of the death penalty being imposed and measures to ensure information collected by Australian authorities is not disclosed where it may be used contrary to the prohibition on torture are also primarily contained in policy documents (see Chapter 17).

Use of artificial intelligence

12.74 Digital Rights Watch expressed concern about inadequate safeguards regulating use of personal information for analysis by artificial intelligence (AI) tools.[687]

12.75 A recent review described the main use case for AI for criminal intelligence as being to 'augment human capacity for tasks such as translation and the generation of intelligence insights from large or complex data sets.'[688] In a review of intelligence agency use of AI, the IGIS described '[t]he most prominent risk' as 'the risk of decisions (autonomous or AI enabled human) being influenced by biased datasets or algorithms, potentially compromising the integrity or accuracy of the decision or operation.'[689]

684 AFP, *Australian Federal Police – Privacy Policy* (Policy, April 2025); ACIC, *Information Handling Protocol* (Policy).
685 HRLC, *Submission 5*, 10; Karen Percy, Media Federal President, MEAA, *Public hearing transcript*, 19 February 2025, 28; Monique Mann, Vice Chair, Australian Privacy Foundation, *Public hearing transcript*, 20 February 2025, 16.
686 Sarah Chidgey, Deputy Secretary, AGD, *Public hearing transcript*, 20 February 2025, 73.
687 Digital Rights Watch went so far as to recommend prohibiting the use of AI to analyse personal information collected as part of a *SLAID Act* warrant: Digital Rights Watch, *Submission 22*, 7.
688 *2024 Independent Intelligence Review*, 79 [13.19].
689 IGIS, *Preliminary Inquiry – Use of Artificial Intelligence by Intelligence Agencies* (Report, 29 May 2024) 5.

12.76 There is some emerging work being done on whole-of-government policy frameworks for the use of AI, although this generally does not apply to the National Intelligence Community (NIC).[690] There is a broader focus within the NIC on developing intelligence community-wide artificial intelligence governance principles and artificial intelligence public messaging principles.[691] The 2024 Independent Intelligence Review recommended that the Monitor undertake a review of the legislative context around the NIC's current use of AI to inform legislative and policy changes.[692]

12.77 This is an emerging area. Whether there is a need for specific statutory or other controls to protect privacy and other rights while analysing data gathered under *SLAID Act* warrants, including the use of AI tools, should be considered as part of a broader review.

A future independent review should consider safeguards on AFP and ACIC analysis of data gathered under *SLAID Act* warrants as part of a broader review of the regulation of AI and related technologies by National Intelligence Community agencies.

Should there be a proportionality test for use, retention and disclosure of personal information?

12.78 In this review, I considered whether there should be an additional general statutory test to ensure information is used, disclosed and retained only where necessary and proportionate to the intrusion on privacy. This type of test could be based on the test recommended by AGD as part of the second stage of proposed reforms to the *Privacy Act*.[693] That test would require that collection, use and disclosure of personal information is objectively 'fair and reasonable in the circumstances' and guided by a non-exhaustive statutory list of considerations, including necessity and

690 See, for example, Commonwealth et al, *National Framework for the Assurance of Artificial Intelligence in Government* (Framework, 21 June 2024) and Digital Transformation Agency, *Policy for Responsible Use of AI in Government* (Policy version 1.1, September 2024) (This policy does not apply to the national intelligence community, including ACIC and AFP in relation to its intelligence functions). The Office of the Australian Information Commissioner also recently released guidance on artificial intelligence and the *Privacy Act*: see Office of the Australian Information Commissioner, *Guidance on Privacy and the Use of Commercially Available AI Products* (Guideline, 21 October 2024). The *Privacy Act* has little or no application to NIC agencies.

691 *2024 Independent Intelligence Review*, 80 (Recommendation 32).

692 *2024 Independent Intelligence Review*, 83 (Recommendation 38). Such a review would currently require a referral under the *INSLM Act*.

693 AGD, *Privacy Act Review Report 2022* (Report, September 2023) 116–20 Proposal 12.1 and 12.2; Australian Government, *Government Response to the Privacy Act Review Report* (Government Response, 2023) 8. The first tranche was implemented by *the Privacy and Other Legislation Amendment Act 2024* (Cth).

proportionality.[694] There were also other suggestions for strengthened controls on proportionate retention.[695]

12.79 A number of civil society submissions supported this or a similar approach.[696] For example, Digital Rights Watch called for 'an overarching obligation … to be implemented … to ensure that personal information collected, used, or disclosed, as part of a warrant issued under the *SLAID Act*, is legitimate, proportionate and balances the right to privacy.'[697]

12.80 Notwithstanding their recommendation in relation to the *Privacy Act*, AGD cautioned this review that such a requirement might 'add significant practical complexity for agencies by adding extra layers of decision making at each step in an investigation' and may result in 'delay, reduce legal certainty and hamper agencies' work.' The department also considered that a standalone 'fair and reasonable' test would be too vague and there is need to provide agencies 'specificity about exactly when information can be used and disclosed,' which can then be subject to oversight.

12.81 I note that a similar requirement to create policies that ensure personal information is retained only 'when it is appropriate and proportionate to the purpose of the relevant function' is imposed on ASIO under the *Guidelines to be Observed by the Australian Security Intelligence Organisation in the Performance of its Functions and the Exercise of its Powers* (ASIO Guidelines).[698] I am unaware of any particular difficulties for ASIO in applying this requirement or for IGIS in oversighting it.

12.82 There is a requirement in the *Intelligence Services Act 2001* (Cth) (*IS Act*) that foreign intelligence agencies covered by that Act only communicate or retain intelligence concerning Australian persons in accordance with written rules made by the relevant responsible Minister. However, that requirement is not equivalent to what is being proposed here – it does not require that the guidelines be limited to proportionate purposes; only that the Minister 'have regard to the need to ensure that the privacy of Australian person is protected as far as is consistent with the proper performance by the agencies of their functions.'[699] The more 'light touch' privacy rules applicable to foreign intelligence agencies should not be taken as a guide to what is appropriate for agencies such as AFP and ACIC, which collect information inside Australia.

694 AGD, *Privacy Act Review Report 2022* (Report, September 2023) 116–20.

695 For example, greater consistency with European Union (EU) General Data Protection Regulation: Philip Glover, *Submission 8*, 7–8. The General Data Protection Regulation came into force in the EU and the United Kingdom on 2 May 2018, updating Directive 95/46/EC and harmonising data protection laws across the EU. See also the *Digital Services Act 2022* (EU) and European Commission, *Regulation of the European Parliament and of the Council: Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts* (Explanatory Memorandum, 21 April 2021).

696 HRLC, *Submission 5*, 10 [4.3]; QCCL, *Submission 6*, 8; AJF, *Submission 7*, 6; IAA, *Submission 16*, 4.

697 Digital Rights Watch, *Submission 22*, 4-5.

698 Attorney-General (Cth), *Guidelines to be Observed by the Australian Security Intelligence Organisation in the Performance of its Functions and the Exercise of its Powers* (Guideline, 4 March 2025) (ASIO Guidelines) 14–15 [4.3]–[4.4]; *ASIO Act* s 8A.

699 *IS Act* s 15.

12.83 In Part 3 and Chapter 11 I have recommended significant changes to the arrangements for issuing *SLAID Act* warrants and the criteria to be considered. One of those is that, in considering the infringement on privacy and the need to protect special categories of information when issuing a warrant, the issuing authority should have regard to the adequacy of internal policies. PIMs will be able to provide feedback to the issuing authorities on the outcome of any IGIS or oversight inspections of the way these policies are being implemented. If these recommendations are accepted, there will be less need for a specific statutory rule that requires use, disclosure and retention of information to be 'fair and reasonable in the circumstances.' Instead, a 'fair and reasonable in the circumstances' test and relevant guidance could be included in agency-specific policies. If these recommendations are not accepted then a statutory requirement that use, disclosure and retention of information to be 'fair and reasonable in the circumstances' should be enacted.

If issuing authorities are required to have regard to the adequacy of agency policies to protect privacy and sensitive categories of information, there will be a reduced need for a statutory requirement that use, disclosure and retention of information be 'fair and reasonable in the circumstances.'

Binding administrative guidance

12.84 Even if the enhanced issuing arrangements and criteria are implemented, there is potential benefit in the relevant Minister issuing some form of binding guidance directed at ensuring that use, disclosure and retention of personal and sensitive information is proportionate. This would provide greater transparency and certainty as to the requirements and would also allow a clear standard for oversight bodies to inspect against. An advantage of placing such detail in binding guidelines rather than legislation is that they can be updated more easily and can contain more detail than is appropriate for legislation.

12.85 The United Kingdom system of binding administrative guidance, referred to as codes of practice, provides a good model for creation and publication of binding administrative guidance setting out the approach the Minister expects law enforcement agencies to take to using covert surveillance powers. Codes of practice are issued by the Secretary of State under the *Investigatory Powers Act 2016* (UK) and currently relate to matters such as bulk acquisition of communications data and equipment interference.[700] These codes must address certain matters such as 'the public interest in the confidentiality of sources of journalistic information' and LPP information.[701]

700 *Investigatory Powers Act 2016* (UK) sch 7 read alongside s 241. See for example, Home Office (UK), *Bulk Acquisition of Communications Data Code of Practice* (Guideline, 6 June 2025).

701 *Investigatory Powers Act 2016* (UK) sch 7 para 2(1)(a),(b).

12.86 Before issuing a code, the Secretary of State must prepare and publish a draft of the code, consider any representations made about it and consult with the Investigatory Powers Commissioner. Codes of practice are binding in the sense that a person must have regard to a code when exercising any functions to which the code relates.[702]

12.87 The Law Council highlighted the United Kingdom approach of issuing binding administrative guidance and said that, among other things, this would enhance safeguards on the life cycle of data. The Law Council said that '[a]dministrative guidance provides a critical role in providing greater certainty regarding the use of these highly intrusive powers' and underlined the importance of 'statutory prompts' for periodic review and public consultation.[703] Angus Murray, of the Queensland Council for Civil Liberties, said the United Kingdom system of requiring public consultation before issuing a code of practice would improve transparency.[704]

> The United Kingdom system of codes of practice provides a good model for creation and publication of binding administrative guidance.

12.88 The guidelines issued to ASIO under s 8A of the *ASIO Act* provide another example of a mechanism for binding administrative guidance to be given, although without the mechanism for public consultation that the United Kingdom model has.[705] These guidelines are public documents issued by the Minister administering the *ASIO Act* and tabled in Parliament. There is a requirement that the Attorney-General be consulted before making the guidelines.[706] Among other things, the document aims to 'provide for an appropriate balance between the privacy and democratic rights of the Australian people and the activities of ASIO'[707] and 'inform the people of Australia of these functions, guidance, standards, accountability, control, oversight and balance.'[708]

12.89 While I think that the United Kingdom model has advantages, including more detailed consultation requirements, the *ASIO Act* approach is adequate. However, I accept that the development of binding administrative guidance around the life cycle of data specifically for *SLAID Act* powers alone would not be a cost-effective proposition. This is a matter that would be more efficiently pursued in the context of holistic ESR. This was supported by the Ombudsman, who observed that 'I query the benefit of developing formal codes of practice with respect to these [SLAID]

---

702 *Investigatory Powers Act 2016* (UK) sch 7 paras 4(1)-(2), 6(1). The codes of practice are also admissible in evidence in any such proceedings and a breach of the code may be considered by a court or tribunal: sch 7 para 6(4).

703 Law Council, *Submission 23*, 17 [39].

704 Angus Murray, Vice President, QCCL, *Public hearing transcript*, 20 February 2025, 17.

705 Directions could be given by the relevant Minister to require compliance with IGIS or Ombudsman guidance on record keeping: *AFP Act* s 37(2); *ACC Act* s 18(1). However, independent oversight bodies should not have to depend on the discretion of an agency Minister in order to obtain information that they require to perform their statutory roles. The *Archives Act 1983* (Cth) was not in any way a substitute for the kind of detailed guidance on the creation and maintenance of records of this type.

706 *ASIO Act* s 8A(1A).

707 ASIO Guidelines, 4 1.6(d).

708 ASIO Guidelines, 4 1.6(e).

powers. However, I see merit in exploring whether codes of practice could be useful in the broader context of electronic surveillance powers.'[709]

Recommendation 16: Further consideration should be given to issuing binding administrative guidance to provide additional protections for the collection, use, retention and disclosure of information, particularly personal and sensitive information.

709 Letter from Ombudsman to INSLM, 31 March 2025.

Part 5. Associated SLAID Act powers – assistance orders and emergency authorisations

In addition to the 3 new warrant types, the *SLAID Act* also included 2 associated powers:

- Emergency authorisations: These enable *internal* approval of data disruption and account takeover in situations of imminent risk of serious violence or substantial property damage where it is not possible to apply for a warrant.
- Assistance orders: These expand the scope of what is authorised under a warrant by *requiring* specified individuals (including those not suspected of committing any offence) to provide assistance in executing the warrant.

These powers are analysed in this Part. The key conclusions are that:

- Emergency authorisations should be retained for AFP, subject to the removal of a limitation that currently prevents an issuing authority from requiring destruction of improperly obtained information. Given its role as an intelligence agency and not a first responder to emergencies, ACIC should not retain *emergency* authorisations. Urgent warrants should remain available to both AFP and ACIC.
- Assistance orders should be retained. However, they should not be used when an industry assistance mechanism would be effective and should be made subject to an express requirement to consider proportionality.

The reporting arrangements for assistance orders are not covered in this chapter. Instead, they are discussed alongside improvements to public and ministerial reporting more broadly in Chapter 15. A current issue with a person subject to an assistance order having the ability to seek legal advice is discussed alongside arrangements for protecting and limiting use and disclosure of information in Chapter 12.

Chapter 13: Emergency authorisations

13.1 One of the roles of police is to respond to emergencies. On occasion it may be necessary for them to exercise powers quickly to avert a serious risk of harm. There are 2 mechanisms in the *SLAID Act* to facilitate a rapid response in situations when it is not practicable to seek a warrant in the normal way:

- an urgent warrant application
- an emergency authorisation.

13.2 Urgent warrant applications are not controversial, as they are determined by an external issuing authority and the standard warrant criteria apply.[710] The difference is that they can be sought remotely by phone or other means and an affidavit is not necessarily required at the time the application is made. The circumstances in which this may be done are noted in Chapter 11.

13.3 Emergency authorisations are more controversial, as they allow for the use of invasive powers without the prior approval of an independent issuing authority. However, emergency authorisations may only be used when there is an *imminent* risk of *serious violence to a person or substantial property damage*, it is *impracticable* to apply for a warrant (including an urgent warrant) and the circumstances are *so serious that the action is immediately necessary*.[711] Emergency authorisations are not available for NAWs This is consistent with their nature as intelligence-gathering warrants.

13.4 This chapter considers emergency authorisations and concludes that, while some relatively minor amendments are required, AFP should retain the existing power but that emergency authorisations are not appropriate for intelligence powers. Use of this type of power is, and should remain, rare.

13.5 The proposed changes to issuing arrangements in Part 3 should make it easier to seek an *urgent* warrant rather than having to rely on an *emergency* authorisation because a dedicated issuing body could make consistent provision for out-of-hours and urgent applications.

710 Note that the *Crimes Act* refers to an 'urgent application' for ATWs (s 3ZZUN(2)), while the *SD Act* refers to a 'remote application' for DDWs and NAWs (ss 27KB, 27KL). They differ in name only, and are jointly referred to as 'urgent warrant applications' in this chapter.

711 *Crimes Act* s 3ZZUX; *SD Act* s 28(1C). Additional criteria apply to emergency data disruption authorisations. These are discussed below.

Actual use of urgent warrants and emergency authorisations

13.6 Between the commencement of the *SLAID Act* and 31 December 2024 (the period for which data was sought in this review) there were no urgent warrant applications.[712] There has been one emergency authorisation. This was an AFP emergency authorisation for an ATW.[713]

There has been only one emergency authorisation for *SLAID Act* powers.

13.7 The very limited use of urgent and emergency authorisations is appropriate. They are intended for use only in very specific circumstances.

13.8 Agencies did not raise any concerns about the statutory criteria for urgent warrants or emergency authorisations. The Law Council of Australia raised some concerns about emergency authorisations for data disruption,[714] and the Australian Information Industry Association also raised concern about the controls on emergency authorisations.[715]

When can an emergency authorisation be sought?

13.9 Before an emergency authorisation can be sought, there are a number of criteria that must be satisfied. First, it must not be practical in the circumstances to apply for a warrant. This includes it being *impractical to apply for an urgent warrant*. Urgent warrant applications can be made remotely, including by telephone or email. Where it is impractical for an affidavit to be prepared, applications can be made without an affidavit.[716] In other words, emergency authorisations are not available if it is possible to contact an issuing authority, including by phone, to seek an urgent warrant.

712 AFP, *Annual Report 2023–24* (Report, 16 September 2024) 150; AFP, *Annual Report 2022–23* (Report, 14 September 2023) 170; AFP, *Annual Report 2021–22* (Report, 12 September 2022) 168; ACIC, *2023–24 Account Takeover Warrant Annual Report* (Report, October 2024) 1; ACIC, *Account Takeover Warrant Annual Report to Minister [1 July 2022 to 30 June 2023]* (Report, August 2023) 1; ACIC, *Crimes Act 1914 – Account Takeover Warrant Annual Report to Minister for the period 4 September 2021 to 30 June 2022* (Report, February 2023) 1; *SD Act Annual Report 2023–24* 27, 30; *SD Act Annual Report 2022–23* 27, 31; *SD Act Annual Report 2021–22* 26, 30.

713 AFP, *Annual Report 2023–24* (Report, 16 September 2024) 150. The emergency authorisation was subsequently approved by an appropriate issuing authority.

714 Law Council, *Submission 23*, 50–1 [188]–[200] Recommendation 24.

715 AIIA, *Submission 12*, 5.

716 *Crimes Act* s 3ZZUN(2); *SD Act* s 27KB. Note that the reference in these provisions to a copy of any affidavit that has been prepared being required to be transmitted only if 'transmission by fax is available' is outdated and should be updated.

13.10 If a system for issuing warrants is effective, it should be extremely rare that an issuing authority cannot be contacted at any time of day or night. The centralised system for issuing warrants proposed in Part 3 should make it easier for AFP and ACIC to contact an issuing authority in urgent circumstances.[717] Nevertheless, it is conceivable that in a truly critical situation police responding to an emergency may not be able to contact an issuing authority and may instead need to gain approval within the internal chain of command.

> Emergency authorisations are not available if it is possible to contact an issuing authority, including by phone, to seek an urgent warrant.

13.11 Second, the officer seeking the emergency authorisation must reasonably suspect that there is an imminent risk of serious violence to a person or substantial damage to property and that disruption of (or access to) data held in the target computer is immediately necessary to deal with that risk. This is a high threshold and it has 3 parts: imminent risk *and* that it is necessary to act immediately *and* that the action is to deal with that risk. For example, emergency authorisations for data disruption and account takeover cannot be sought to preserve evidence that may otherwise be lost.[718] They can only be sought to deal directly with an imminent risk of serious violence or substantial damage to property. The officer must also reasonably suspect that the circumstances are so serious and the matter is of such urgency that the proposed disruption or account takeover is warranted.[719]

> There needs to be imminent risk of serious harm or damage; it must be necessary to act immediately; and the action must be to deal with that risk.

717 I have been advised that in the UK when telecommunications data access approvals were centralised in IPCO the result for police and other agencies that use those powers was that authorisations were able to be obtained faster. The centralised system in the UK has a 24/7 roster of dedicated issuing authorities and a clear process for prioritising urgent requests. Previously these approvals were done internally by police and other agencies.

718 Other types of less invasive surveillance power can be used to preserve evidence on the basis of an emergency authorisation for a limited set of offences (see *SD Act* s 30). This emphasises that data disruption and account takeover powers are extraordinary and are not intended to be used for this purpose.

719 *Crimes Act* s 3ZZUX(1)(c); *SD Act* s 28(1C)(c).

13.12 For data disruption authorisations there is an additional criterion. The officer applying for the warrant must reasonably believe there are no alternative methods that law enforcement officers could have used to help reduce or avoid that risk and that would be likely to be as effective as disruption of data held in the target computer.[720] This is consistent with the nature of DDWs as a method of 'last resort.'

13.13 There are also practical limits to seeking an emergency authorisation to disrupt data or take over an account. In evidence to this review, AFP and ACIC emphasised that highly specialised staff and equipment are needed to execute *SLAID Act* powers. They said that extensive planning and testing goes into ensuring that operations are effective and that unintended consequences are avoided.[721] This is particularly so for data disruption. AFP noted 'the need to adequately consider risks and develop plans to ensure a DDW can be executed effectively, without negatively impacting the data of innocent persons' means that 'an emergency DDW would only be utilised in extenuating circumstances.'[722]

When can an emergency authorisation be granted?

13.14 An emergency authorisation can be granted where the relevant internal decision-maker is satisfied that there are 'reasonable grounds' to support each of the criteria that the officer applying for the warrant must meet reasonably suspect exist (see paragraphs 13.09 to 13.12 above).

13.15 In addition, before authorising data disruption the decision-maker must consider the likely extent of interference with lawful use of a computer and whether the likely impact is proportionate to the risk of serious violence or substantial damage.[723]

13.16 A written record of the authorisation needs to be made as soon as possible. Within 48 hours of an emergency authorisation being granted, an application must be made to an issuing authority for approval of the authorisation.[724] At that point a warrant can also be sought if there is a requirement to continue the operation. There is further discussion later in this chapter about the matters that need to be considered if a warrant is issued following an emergency authorisation.

720 *SD Act* s 28(1C)(ba). Note that emergency data disruption authorisations are also subject to a statutory condition intended to ensure that they are not exercised in a way that causes unnecessary damage or permanent loss of property, digital currency or money (s 28(5)).
721 AFP, *Submission 18,* 4 [23]; Rob Nelson, Commander, AFP, *Public hearing transcript*, 20 February 2025, 38–9; ACIC, *Submission 17*, 3, 9; Heather Cook, CEO, ACIC, *Public hearing transcript*, 20 February 2025, 42–3.
722 AFP, *Supplementary response 29*, 2.
723 *SD Act* s 28(4A).
724 *Crimes Act* ss 3ZZUY, 3ZZVA; *SD Act* ss 31, 33.

Should emergency authorisations be permitted?

13.17 As they are quite different types of powers, the need for emergency authorisation powers for data disruption, account takeover and network activity need to be considered separately.

Data disruption

13.18 AFP submitted that, while 'in most circumstances it would not be appropriate for AFP to seek an emergency DDW,' an emergency authorisation must be available so that AFP can 'ensure we can be agile when a critical need arises.'[725]

13.19 The Law Council of Australia made 2 interrelated points about data disruption authorisations. First, 'data disruption is a materially different power' from electronic surveillance, so it should not be accepted that the existing framework for internal authorisation of surveillance powers is automatically suitable for data disruption. Second, data disruption should be excluded from internal authorisation because it has 'the potential to cause much greater harm to non-suspects than surveillance alone.'[726] As discussed in Chapter 2, I agree that data disruption is a materially different power and that it has the potential to cause greater harm, including to non-suspects, than surveillance.

13.20 Police are first responders. In a situation where there is imminent risk of serious violence to a person or substantial damage to property and it is necessary for police to act immediately to deal with that risk, they should have access to a rapid means to authorise the use of appropriate powers. Emergency authorisations need appropriate safeguards, including the high threshold and current additional considerations that must be satisfied for a data disruption authorisation. Some minor adjustments to the scheme are proposed later in this chapter. With those safeguards, in my view it is appropriate that AFP retain the ability to internally approve the use of data disruption powers in an emergency.

> AFP should retain the ability to internally approve the use of data disruption powers in an emergency.

13.21 The situations in which AFP would need to use this type of power are very rare and they would probably be part of broader police response to life-threatening or critical infrastructure damage incidents. I am mindful that most data disruption techniques require considerable planning and preparation before they can be deployed and that in such cases there would be time to obtain a regular warrant or an urgent warrant. Therefore, only a limited range of techniques could be deployed immediately in an emergency.

725 AFP, *Supplementary response 29*, 2.
726 Law Council, *Submission 23*, 50 [188].

13.22 For the reasons discussed in Chapter 5 I have recommended that ACIC not retain DDWs. A consequence of that recommendation is that ACIC would also not be able to seek emergency authorisations for data disruption. If that recommendation is not accepted then, in my view, emergency authorisations for ACIC should still be repealed. The ACIC Review makes clear that ACIC is not a 'first responder' for serious harm and critical damage emergencies, which are the only situations where emergency authorisations can be utilised. There should be administrative arrangements in place for ACIC to pass information to and cooperate with police quickly if they gather intelligence about high-risk situations, whether they arise in the physical or the cyber domain.[727]

If ACIC retains DDWs, it should not retain the ability to internally authorise data disruption.

Account takeover

13.23 AFP gave the example of using account takeover powers in the execution of a computer access or search warrant. AFP indicated that it may be necessary to use an emergency authorisation where AFP finds the suspect is using accounts that are additional to those identified in an ATW that has already been issued.[728] That type of situation would not meet the threshold for an emergency authorisation because the purpose would be to obtain evidence that may otherwise not be able to be seized. There would also need to be an imminent risk of serious violence to a person or substantial damage to property and the takeover of the account must be immediately necessary to deal with that risk. It would also need to be established that it was not practicable to contact an issuing authority (including by phone) for an urgent warrant during the execution of the computer access or search warrant.[729] In any case, the introduction of named-person ATWs, as recommended in Chapter 6, will address this scenario.

13.24 Nevertheless, there may be rare situations in which there is an imminent risk of serious violence or substantial property damage and it is necessary for police to act rapidly by taking over an account to address that risk. This may be in the context of a wider police operation – for example, if an account takeover could be expected to assist in promptly locating a hostage or missing child who is at imminent risk of serious harm. With appropriate safeguards AFP should retain the ability to internally approve the use of data disruption powers in an emergency.

727 The *ACIC Review* recommended the implementation of a formal mechanism for ACIC to access police support in the exercise of its functions: *ACIC Review* 32–4 Recommendation 10. This recommendation was agreed to by government: *Government Response to the ACIC Review* 8.

728 Rob Nelson, AFP, *Public hearing transcript*, 20 February 2025, 34–5.

729 *Crimes Act* s 3ZZUX.

AFP should retain the ability to apply for emergency account takeover authorisations.

13.25 The case is less clear for ACIC. As discussed in Chapter 5, I have recommended that ACIC retain the ability to utilise ATWs but that, in line with the recent ACIC Review, the ATW should be altered so that it can be obtained for intelligence purposes rather than evidence collection. This is consistent with the proposed shift in the role of ACIC to be 'positioned as Australia's national criminal intelligence agency.'[730]

13.26 ACIC has not used any ATWs, but it said that their possible future use is more likely to be through a remote account takeover, rather than during a physical search as described by AFP.[731] Given this type of remote access as part of an intelligence operation is going to require some planning and preparation, this should allow at least an urgent application for a warrant to be made.

13.27 This being the case, and consistent with the fact that ACIC is not a 'first responder' to situations involving serious harm or serious property damage, I do not consider it necessary for ACIC to retain the capacity to internally authorise emergency use of account takeover. This will particularly be the case if recommendations of the ACIC Review concerning ACIC's criminal intelligence role are implemented.[732]

ACIC should retain the ability to seek urgent ATWs. However emergency account takeover authorisations should not be available to ACIC.

Network activity

13.28 NAWs can be obtained from an external issuing authority on an urgent basis, but there is currently no provision for an internal emergency authorisation for a NAW. NAWs are intended for intelligence-gathering operations. These are usually longrunning operations that require significant planning and resources. NAWs are not, and should not be, regarded as an emergency response tool. Other emergency authorisations, including for computer access and use of surveillance devices, already exist and are the appropriate tool for targeted emergency responses by law enforcement authorities.

730 *ACIC Review* 7.

731 ACIC, *Submission 17*, 6; INSLM, *Summary of private hearing – ACIC*, 11 March 2025, 2–3. Contrast with AFP, *Submission 18*, 6 [37]; Rob Nelson, Commander, AFP, *Public hearing transcript*, 20 February 2025, 34–5.

732 See particularly *ACIC Review* Recommendations 1–4 and 9–11, each of which was agreed to by government: *Government Response to the ACIC Review* 5–6, 8–9.

Introduction of an emergency network activity authorisation is unnecessary and would be inappropriate.

13.29 Neither AFP nor ACIC suggested that there was a need to introduce emergency network activity authorisations.

Recommendation 17: The scheme for emergency authorisations should be amended so that:

(a) Emergency authorisations are not available to ACIC.

...

Are changes needed to the scheme for emergency authorisations?

13.30 Having concluded that the existence of an internal emergency authorising mechanism is appropriate, it is necessary to consider if any changes to the scheme are required.

Should the definition of 'emergency' be expanded?

13.31 The types of emergencies for which data disruption or an account takeover authority can be sought are an imminent risk of serious violence to a person or substantial damage to property. No proposal was put forward to this review that this should be expanded.

13.32 However, I am aware that the 2019 Comprehensive Review recommended that other law enforcement electronic surveillance powers be available to address specific emergenceis:

- prevent or lessen imminent threats to life or of serious harm or damage to property
- locate and investigate suspected kidnappings
- locate missing persons
- recover a child subject to a child recovery order.[733]

[733] *2019 Comprehensive Review* vol 2 331 Recommendation 101. The government accepted this recommendation: *Government response to the 2019 Comprehensive Review* 30.

13.33 As discussed elsewhere in this report, data disruption is an extraordinary power that is not akin to electronic surveillance. Account takeover is also more rights-intrusive than surveillance alone. For this reason, there would have to be a very strong case for expanding their use beyond imminent risk of serious violence to a person or substantial damage to property – a category that would already include serious risk to the life or safety of kidnapped or missing persons, including children. No such case was put forward, and great caution should be exercised in expanding the internal authorisation of extraordinary powers. At this point I see no reason to expand the availability of emergency authorisations for account takeover and data disruption. Urgent warrant applications also remain available, as do emergency authorisations for 'ordinary' surveillance.

There is no reason to expand the availability of emergency authorisations for account takeover and data disruption.

Internal authorising officers

13.34 For AFP, authorising officers are the Commissioner, Deputy Commissioner and any senior executive AFP employee authorised by the chief officer. For ACIC, appropriate authorising officers are the Chief Executive Officer (CEO) and any executive level member of staff the chief officer authorises.[734] This is inconsistent and leaves open the theoretical possibility that, if ACIC retains emergency authorisations, the CEO of ACIC could confer authority to grant emergency authorisations on an individual who is not a senior executive service (SES) level employee.[735] ACIC has not actually delegated below SES level and did not suggest that it would be necessary or appropriate to do so.

13.35 If, contrary to Recommendation 17, ACIC retains the authority to issue any type of emergency authorisation, it should be formally restricted to the CEO, Deputy CEO and SES level staff. My expectation is that both AFP and ACIC would only delegate below the Deputy Commissioner / Deputy CEO level if there were sound operational reasons for doing so and the SES staff selected had appropriate training and experience.

If ACIC retains emergency authorisations to disrupt data or take over accounts, authority to issue emergency authorisations should be limited by statute to the equivalent of SES level staff and above.

734 *SD Act* s 6A(6) table item 15.

735 Law Council, *Submission 23*, 51 [189]; Law Council, Submission No 21 to PJCIS, Parliament of Australia, *Review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (9 March 2021) 87 [273]–[276].

13.36 AGD supported such amendments to 'promote consistency' and to 'assist to sustain public confidence.'[736]

Approving emergency authorisations and subsequent warrant applications

13.37 Within 48 hours of an emergency authorisation being granted, an application must be made to an issuing authority to 'approve' the authorisation. The matters an issuing authority is required to consider are comprehensive, but they recognise that emergency authorisations are granted in emergency circumstances and on the basis of specific criteria. Hence, the test is framed in terms of whether it was reasonable to suspect there was an imminent threat to life etc. at the time the emergency authorisation was granted and whether the action proposed may have helped reduce the risk.[737] The matters the issuing authority must consider when deciding whether to retrospectively approve an emergency are appropriate. I do not recommend any changes, and agencies did not seek any.

13.38 A matter that is distinct from the retrospective approval of an emergency authorisation is whether the disruption or account takeover should continue. It may be that the emergency has been resolved and there is no need to continue it or that a warrant is sought to continue the activity.

13.39 The information that must be provided when seeking a warrant (including an urgent warrant) is more comprehensive than what is required for an emergency authorisation. At the moment is it not entirely clear that an application for a warrant following an emergency authorisation must include the same information as other warrant applications. This ambiguity arises because the legislation simply says that, after considering an emergency authorisation, the issuing authority may issue a warrant 'as if the application for the approval [of the emergency authorisation] were an application for a warrant.'[738] This may result in insufficient information being provided to enable a warrant application to be properly considered.

13.40 The introduction of a public interest monitor (PIM) and an express duty of candour, as recommended in Part 3, would resolve this concern. If these recommendations are not accepted then a clarifying amendment would be desirable.

736 AGD, *Submission 20*, 19.
737 *Crimes Act* ss 3ZZVB, 3ZZVC; *SD Act* ss 34(1B), 35B. Also see comments on underpinning policy in AGD, *Submission 20*, 18–9.
738 *SD Act* ss 35B(2)(a), 35B(3)(b); *Crimes Act* ss 3ZZVC(2)(a), 3ZZVC(3)(b).

Remedy for actions taken under an emergency authorisation

13.41 The Australian Human Rights Commission and the Law Council of Australia both echoed a recommendation of the PJCIS in submitting that there should be some form of remedial action available to people if they are affected by actions taken under an emergency authorisation that the issuing authority does not subsequently approve.[739] The right to an effective remedy is an issue for *SLAID Act* powers more generally and is discussed in Chapter 17. For emergency authorisations there are broadly 3 options for a 'remedy':

- The affected individual can pursue a civil action. However, as discussed in Chapter 17, the covert nature of *SLAID Act* warrants makes this an unlikely option. The same can be said for remedies under administrative schemes such as the Scheme for Compensation for Detriment caused by Defective Administration.
- The Ombudsman may identify a concern with an emergency authorisation and, after an investigation, may recommend some form of remedial action. As discussed in Chapter 16 and Chapter 17, this kind of review is important in relation to covert powers, but it is not strictly a 'remedy' for an individual.
- The issuing authority can make certain types of orders as part of the process of retrospectively approving (or not approving) the emergency authorisation. These are discussed below.

13.42 When considering an application to retrospectively approve an emergency authorisation, the issuing authority currently has discretion to order that information obtained from or relating to the use of powers under the authorisation is dealt with in a specified manner. However, there is a limitation that prevents the issuing authority from requiring destruction of the information.[740]

> While not a complete remedy for inappropriate action, the authority to give a binding order as to how information is to be dealt with is an important protection.

13.43 I am concerned about the current limitation preventing destruction of information. I recognise that there are situations where it would be inappropriate to destroy improperly obtained information. Foremost amongst those is that the Ombudsman or another body may need the information as part of an investigation of how the information came to be collected.[741] There may also be cases where the evidential value of the information is so high that it should be retained, even though there

739 AHRC, *Submission 21*, 16 [54]–[55]; Law Council, *Submission 23*, 51 [190]; *PJCIS SLAID Report* 136 [6.73].
740 *Crimes Act* s 3ZZVC(4); *SD Act* s 35B(4).
741 This is the type of scenario envisaged by the *Revised Explanatory Memorandum* 60 [253].

was some irregularity in the emergency authorisation.[742] Nevertheless, there may be situations where, in all the circumstances, there is no valid reason to permit retention of the material. I see no reason why an independent issuing authority, particularly one with the experience of a retired judge and the benefit of submissions from a PIM as well as the agency, would not be able to weigh all the factors and make an appropriate order.

Recommendation on emergency authorisations

Recommendation 17: The scheme for emergency authorisations should be amended so that:

(a) Emergency authorisations are not available to ACIC.

(b) The limitation preventing an issuing authority from ever requiring the destruction of information should be removed.

742 This is comparable to the discretion to allow the admission of improperly or illegally obtained evidence in a proceeding where the desirability of admitting the evidence outweighs the undesirability of admitting evidence obtained in that way – see, for example, *Evidence Act 1995* (Cth) s 138.

Chapter 14: Assistance orders

14.1 An assistance order requires a specified a person to provide 'any information or assistance that is reasonable and necessary' to assist in execution of the warrant.[743] These orders are made by an independent issuing authority in conjunction with a warrant or to support an emergency account takeover authorisation.[744] Failure to comply with an assistance order is a serious offence.[745] Assistance orders are not limited to people who are reasonably suspected of engaging in criminal activity – for example, they can be directed at system administrators.

14.2 This chapter considers when an assistance order can be made and who can be subject to one. The key finding is that, although no assistance orders have been used for *SLAID Act* warrants, they should be retained. However, it is recommended that additional safeguards be implemented. For example, assistance orders should not be used to seek assistance available under an industry assistance framework; proportionality should be an express consideration in the issuing of any *SLAID Act* assistance order; and a person subject to an order should not be barred from seeking legal advice on that order.

When are assistance orders likely to be used?

14.3 The legislation does not specify what sort of assistance can be required beyond the assistance being 'reasonable and necessary.' The examples given by agencies as to when assistance orders may be utilised generally suggest that the orders would require a person who is otherwise unlikely to cooperate to provide assistance in the execution of the warrant. For example:

- The subject of the warrant could be required to provide 'a password, PIN code, sequence or fingerprint necessary to unlock a computer or account that is the subject of a warrant.'[746]
- A member of a criminal network that has established secure communications could be required to use their knowledge of the secure communications system to assist AFP in gaining access to data.[747]

743 *Crimes Act* s 3ZZVG(1); *SD Act* ss 64A(1), 64B(1).
744 As a practical matter it does not seem possible that an assistance order would be sought from an issuing authority for an emergency authorisation granted (internally) for an ATW given that one of the criteria for issuing an emergency authorisation is that it is not practicable to contact an issuing authority to grant a warrant.
745 In the case of a *SLAID Act* warrant the penalty is up to 10 years imprisonment, 600 penalty units or both: *Crimes Act* s 3ZZVG(3); *SD Act* ss 64A(8), 64B(3).
746 AGD, *Submission 20*, 20.
747 AFP, *Submission 18*, 8 [48].

- A system administrator who is not involved in alleged offending conduct but who knows how to access a forum hosted on a web service could be required to assist AFP or ACIC by providing access to the forum.[748]
- A person could be required to give assistance in the execution of a warrant in urgent circumstances where there is not time to use covert means, even though this will mean that the person who is the subject of the warrant and the order will become aware of its existence.[749]

14.4 It should be noted that, while the examples given above illustrate the type of assistance that AFP and ACIC have in mind, the legislation allows for 'any' information and assistance to be required, provided it is reasonable and necessary for warrant execution.[750] The order does not need to specify the type of assistance that has to be provided. The question of what is 'reasonable and necessary' to execute the warrant is an objective test that must take account of all the circumstances.

No assistance orders have been sought

14.5 No assistance orders have been sought for ATWs, DDWs or NAWs.[751] This means that the examples above are hypothetical.

14.6 AFP noted that to date it has generally used ATWs in conjunction with other warrants such as search warrants and that, in these situations, an order obtained for the search warrant may mean it is not necessary to seek a separate assistance order for an ATW:

> As ATWs have (to date) generally been used where section 3E warrants are being executed there is often not a need to seek both a 3LA order and a *SLAID Act* assistance order in advance of overt activity. Nevertheless, were an ATW to be used separately to a section 3E search warrant the ability to seek an assistance order may prove beneficial.[752]

14.7 Although no assistance orders have been sought under the *SLAID Act* provisions I am satisfied that there are situations, albeit rare situations, where it is foreseeable that the power may be needed in order to give effect to a warrant. This makes it necessary to consider whether the present safeguards – for example, those on who can be the subject of orders and what thresholds must be met for an order to be made – are sufficient.

748 Revised Explanatory Memorandum 71 [328]–[329].
749 Revised Explanatory Memorandum 71 [328]–[329].
750 *Crimes Act* s 3ZZVG(1); *SD Act* ss 64A(1), 64B(1).
751 Copies of warrants and reports as at 11 February 2025 were produced by both AFP and ACIC in response to notices under s 24 of the *INSLM Act*.
752 AFP, *Submission 18*, 8–9 [49].

Who can be subject to an assistance order?

14.8 A wide range of individuals may be affected by assistance orders. For all *SLAID Act* warrants an assistance order can sought for a specified person who is:

- reasonably suspected of having committed the offence(s) in respect of which the warrant or emergency authorisation was issued
- the owner or lessee of the target computer or holder of the target account
- an employee or contractor of the owner or lessee of the target computer or holder of the target account
- a person who uses or has used the target computer or account
- a person who is or was a system administrator for a system that includes the target computer or the electronic service to which the account relates.[753]

14.9 A distinction can be made between those who are suspected of some wrongdoing – including committing the offence that is the subject of the warrant or knowingly or recklessly facilitating the commission of that or a related offence – and those who are not suspected of any wrongdoing.

14.10 Even though it might assist in executing a warrant, it will rarely be proportionate to subject a person who is not suspected of any wrongdoing to an order that carries with it a 10year penalty for noncompliance, especially if the person is willing to voluntarily cooperate with police or where an alternative scheme or mechanism for obtaining assistance is available. The absence of an express requirement to consider proportionality in the case of some assistance is concerning. I return to it below.

14.11 As a general proposition, those who are genuinely providing voluntary assistance in the execution of a warrant, including industry bodies and individuals, should be supported by targeted indemnities, rather than being 'voluntarily' subjected to a broad order with a 10year penalty.[754] Questions as to whether voluntary assistance will be forthcoming is a matter of fact to be determined by the issuing authority in individual cases and goes to the necessity and proportionality of an order.

753 *Crimes Act* s 3ZZVG(2)(b); *SD Act* ss 64A(6A)(b), 64B(2)(e).

754 See, for example, *ASIO Act* s 21A. See also the scheme that applies to controlled operation under pt IAB of the *Crimes Act*.

Assistance orders and industry assistance

14.12 During the PJCIS review of the SLAID Bill, and again during this review, industry bodies raised concerns that assistance orders might be used to circumvent the procedures and safeguards that apply to requests for industry assistance under other schemes.[755] Specifically, an assistance order might be served on an employee or contractor of a carrier or carriage service provider (CSP) to effectively force assistance from the carrier or CSP itself.[756]

14.13 Schemes for assistance such as that introduced by the *TOLA Act* provide a range of specific safeguards for industry that are not present in the assistance order provisions. Very briefly, these include the exclusion of requests that would introduce a systemic vulnerability, consultation requirements, immunity from civil liability for good faith assistance, and express requirements relating to feasibility and proportionality.[757]

14.14 In response to concerns that the PJCIS expressed about assistance orders being available where an industry assistance scheme was more appropriate, an amendment was made to the Revised Explanatory Memorandum to assert that:

> The intent … is not to allow law enforcement to compel assistance from industry (for example a telecommunications company) … Assistance provided by industry is governed by the industry assistance framework introduced by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*. The [assistance order] provision does not replicate [that framework], or allow the AFP or ACIC to circumvent the protections in that framework.[758]

14.15 AGD and AFP confirmed that this limitation reflects the policy intention and current practice.[759] However, there is currently nothing in the legislation that clearly reflects this.[760]

---

755 *PJCIS SLAID Report* 35–8 [2.93]–[2.103], 140 [6.86]–[6.88]; AIIA, *Submission 12*, 3; IAA, *Submission 16,* 4.

756 IAA, *Submission 16,* 4; Sophia Joo, IAA, *Public hearing transcript*, 19 February 2025, 36–7; Siew Lee Seow, AIIA, *Public hearing transcript*, 19 February 2025, 37.

757 *Telecommunications Act 1997* (Cth) ss 313(5)–(6), 317JAA, 317JC, 317P, 317RA, 317V, 317ZAA, 317ZG–317ZH; IAA, *Submission 16*, 4.

758 *Revised Explanatory Memorandum* 71 [326], 121 [632], 195 [1147]. But see *PJCIS SLAID Report* 142 [6.94] Recommendation 22.

759 AGD, *Submission 20,* 20; AFP, Submission No 6.1 to PJCIS, Parliament of Australia, *Review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (April 2021) 16 [37]. Evidence was given to this review that ACIC plans to use the *TOLA Act* industry assistance provisions to execute *SLAID Act* warrants: ACIC, *Submission 17*, 3.

760 See *Crimes Act* ss 3ZZVG(2)(b)(iii)–(iv), 3ZZVG(2)(b)(vi); *SD Act* ss 64A(2)(d)(iii)–(iv), 64A(2)(d)(vi), 64B(2)(e)(iv)–(v), 64B(2)(e)(vii), which specifically refer to an assistance order being granted in relation to an employee or contractor of the owner of a computer or a system administrator for a system including the computer.

14.16 In my view it should not be possible to use assistance orders to effectively compel the assistance of a carrier or CSP. This type of assistance should be sought through the usual industry assistance mechanisms. If other schemes, such as voluntary assistance, are available, it may not be necessary or proportionate to issue an assistance order. As discussed below, a criterion of proportionality currently applies to assistance orders for data disruption but not account takeover or network activity.

In the absence of a requirement to be satisfied an assistance order for a NAW or ATW is proportionate, it should be put beyond doubt that assistance orders cannot be used to compel the assistance of a carrier or CSP. This type of assistance should be sought through the usual industry assistance mechanisms.

Should proportionality be part of the test for an assistance order?

14.17 The main issuing criteria that an issuing authority be satisfied of before approving an application for an assistance order are summarised in Table 5 below. There are differences between NAWs, ATWs and DDWs, the most significant being that only assistance orders for DDWs require an issuing authority be satisfied that an assistance order is justifiable and proportionate. DDW assistance orders also require consideration of whether the order is 'reasonable and necessary to execute the warrant.' There is overlap between these requirements: an order that was not reasonable and necessary to execute the warrant would not be proportionate.

14.18 Table 5 highlights that, unlike for DDWs, the criteria that issuing authorities must be satisfied of for NAWs and ATWs do not expressly require the issuing authority to consider whether an order is 'reasonable and necessary,' 'justifiable and proportionate,' or any other similar threshold. The express criteria specific to the order are instead limited to satisfaction that the subject of the order has knowledge that will assist and has one of the relations to the targeted computer or impugned conduct.[761]

761 *Crimes Act* s 3ZZVG(2)(b)–(c); *SD Act* ss 64A(6A)(b)–(c).

Table 5 – Main criteria for granting assistance orders under SLAID Act warrants and authorisations

Criteria the issuing authority must be satisfied of	DDW[762]	NAW[763]	ATW[764]
Person has relevant knowledge and one of the listed relations to the computer or conduct	✓	✓	✓
Assistance order is reasonable and necessary to enable warrant execution	✓	✗	✗
Assistance order is justifiable and proportionate	✓	✗	✗

14.19 Aside from the criteria the issuing authority applies, there are no express considerations a law enforcement officer must consider or be satisfied of *before* applying for an assistance order. For NAWs and ATWs, the only express consideration of proportionality is the requirement that the assistance a person is asked to provide under an order is limited in any case to that which is 'reasonable and necessary' to give effect to the warrant or authorisation under which the order was sought.

14.20 The Internet Association of Australia submitted that the current assistance order provisions do not contain adequate safeguards or oversight. It recommended that express requirements be introduced to require issuing authorities to consider the privacy impacts of an assistance order and whether these types of requests are justified and proportionate.[765] Privacy impact is an example of a matter that would currently need to be considered in issuing a DDW assistance order (as it goes to proportionality) but not necessarily an assistance order for an ATW or NAW. Privacy may be particularly relevant to biometrics.

762 *SD Act* s 64B(2).
763 *SD Act* s 64A(6A).
764 *Crimes Act* s 3ZZVG(2).
765 IAA, *Submission 16*, 4.

In deciding whether to issue an assistance order for an ATW or NAW, the issuing authority is not currently expressly required to consider whether the object of the order is proportional to the impacts on the person from whom it will compel assistance (or anyone else).

14.21 Requiring that intrusive powers be available only where they are proportionate is an important safeguard. An assessment of proportionality takes into account the seriousness of the crime being investigated, expected utility of the assistance, impact on the individual and the availability of any other effective mechanisms to enable execution of the warrant.

14.22 While the exact wording is a matter for drafters, the criteria to be satisfied before an assistance order is granted should make clear that orders can only be granted where it is proportionate to make the order in the circumstances.

Should the type of assistance have to be specified in the order?

14.23 As noted earlier, there is currently no express requirement to specify in the order itself the type of assistance that must be rendered. This is presumably because in some cases the exact type of assistance will not be known until the warrant is executed. When it is executed and the person is asked to provide assistance, that assistance has to be 'reasonable and necessary.'[766] Whether something is 'reasonable and necessary' at that moment will depend on the facts and circumstances at the time the request for assistance is made. In some cases this will be fairly clear; in others it may not. This goes to ensuring the person is not prevented from obtaining legal advice on an assistance order, as discussed along with rules controlling information associated with *SLAID Act* powers in Chapter 12.

14.24 Where it is known in advance, the nature of the assistance the applicant intends to seek may also go to assessing the proportionality of issuing the order in the first instance. In some cases it may be appropriate for the issuing authority to place conditions on an assistance order. For example that biometric information not be retained by an agency. There is currently no express authority to do this, although the general rule in s 33(3A) of the *Acts Interpretation Act 1901* (Cth) would potentially permit an issuing authority to limit the order to only some types of assistance or classes of assistance.[767] If there is any doubt about this, it should be put beyond doubt that issuing authorities can place limits or conditions on assistance orders.

766 *Crimes Act* s 3ZZVG(1); *SD Act* ss 64A(1), 64B(1).
767 *Acts Interpretation Act 1901* (Cth) s 33(3A).

Recommendation on assistance orders

Recommendation 18: The scheme for assistance orders should be modified so that:

(a) Assistance orders are only able to be issued when it is proportionate to do so.

(b) Issuing authorities have express authority to place limits or conditions on assistance orders.

14.25 In making this recommendation I am mindful that the principles underpinning the recommendation may apply to the broadly similar assistance order regime that applies to a range of other warrants, including under the *SD Act* and the *Crimes Act*.[768]

[768] See, for example, *SD Act* ss 64A(2)–(7); *Crimes Act* s 3LA; *ASIO Act* s 34AAD.

Part 6. Reporting and oversight

Oversight in the form of ministerial accountability, public reporting and inspection and review by independent bodies are all critical parts of ensuring that special powers authorised under warrants, assistance orders or emergency authorisations are used in a proper way and that the public can trust that this is the case.

Ministerial reporting should be maintained, and in some respects enhanced. For example, instead of annual reporting on individual ATWs, it should be done at the end of each warrant. There is also opportunity to improve the quality and consistency of reporting.

Public reporting also needs to be enhanced. While there will always be limits on what can be reported publicly, there is certainly additional statistical information that can and should be reported. There is benefit in an annual statement that provides qualitative information about how the use of each type of warrant has contributed to investigating or disrupting serious crime.

Currently, oversight of the use of *SLAID Act* powers is divided between IGIS and the Ombudsman. IGIS has a more flexible inspection remit that allows consideration of 'propriety' as well as legality. The narrower and more prescriptive scheme for Ombudsman inspections of *SLAID Act* warrants should be replaced by a more flexible approach, similar to that for IGIS.

Because of the overlap between the work of IGIS and the Ombudsman on *SLAID Act* warrants, it is important that they are able to effectively share information. Oversight can also be enhanced by access to advice from the technical advisory panel. Some improvements to public reporting of oversight findings is also recommended.

Good record keeping and appropriate notification requirements are both important for effective oversight. Currently, the statutory scheme for these is complex and inconsistent. A better approach would be to have a statutory scheme that allows for detailed and binding administrative guidance to be given on these matters, following appropriate consultation.

Chapter 15: Reporting

15.1 AFP and ACIC are required to prepare 2 types of reports on their use of *SLAID Act* powers:

- reporting to the relevant Minister, including about the use and effectiveness of individual warrants and emergency authorisations
- annual public reporting containing high-level statistical information.

These reporting requirements are directed to different objectives.

15.2 Comprehensive reporting about the use of special powers is an important part of ministerial responsibility and accountability to the Parliament. As these reports are also provided to IGIS and the Ombudsman, this reporting also has a practical role in the oversight process.

15.3 Public annual reporting on the use of invasive and covert powers increases transparency about the effective and proportionate use of these powers. For example, it provides information about how frequently (or infrequently) powers are used and what they are used for. This reporting is necessarily less detailed than that provided to the Minister.

15.4 Submitters expressed a range of views about the current effectiveness of both forms of reporting in meeting these objectives, including about whether it is more useful for the Minister (as compared to oversight agencies) to receive individual warrant reports and the adequacy of current public annual reporting in demonstrating effective and proportionate use of *SLAID Act* powers.

15.5 This chapter explains the need for some changes to both requirements to ensure that they remain fit for purpose and that reports are provided in a timely manner.

Ministerial reporting

15.6 The *SD Act* requires each agency to report to the relevant Minister on the details of a DDW or NAW (and any emergency authorisation) as soon as practicable once the warrant or authorisation has ceased to have effect.[769] For ATWs, there is no requirement to report to the Minister after an individual warrant or emergency authorisation has ceased. Instead, an annual report on all ATWs and authorisations sought in the year must be provided to the Minister and the Ombudsman.[770]

769 During this review, there was a change to the responsible Minister from the Attorney-General to the Minister for Home Affairs – on 13 May 2025 for DDWs and NAWs and for ATWs on 26 June 2025. Governor-General of the Commonwealth of Australia, *Administrative Arrangements Order* (13 May 2025); Governor-General of the Commonwealth of Australia, *Administrative Arrangements Order* (26 June 2025).

770 *Crimes Act* s 3ZZVL. A public annual report is also provided for in s 3ZZVM. This is consistent with other warrants in the *Crimes Act*, such as the delayed notification search warrant: see *Crimes Act* s 3ZZFB.

15.7 For DDWs and NAWs, reports on individual warrants are required to include, among other matters:

- the period during which data was accessed (or disrupted for DDWs) and the name, if known, of any person whose data was accessed (or disrupted for DDWs)
- details of compliance with any conditions attached to the warrant and the benefit of the warrant in frustrating criminal activity (for DDWs) or contribution to preventing, detecting or frustrating a relevant offence (for NAWs).

15.8 The report must also address the number of, and reasons for, any extensions or variations.[771]

15.9 For ATWs, AFP and ACIC must submit an annual report to the Minister and the Ombudsman that sets out certain things that occurred during the previous 12 months. This covers broadly similar matters to those required for DDWs and NAWs, but it is a single report provided once a year rather than separate reports on each warrant.[772] There are some inconsistencies in the reporting requirements for all 3 *SLAID Act* warrant types that need to be addressed. These are discussed later in this chapter.

15.10 In this review, 3 main issues were raised about the efficacy of ministerial reporting:

- how useful it is for AFP and ACIC reports on individual warrants to be provided to the Minister, as compared to oversight agencies
- the scope and content of reporting requirements
- timeliness of reporting.

771 *SD Act* ss 49(2D)(d)(iii), (iv), (vi), (viii), 49(2E)(b)(iii), (iv), (vii), (x), 49(2D)(e), 49(2E)(c).
772 *Crimes Act* s 3ZZVL(1)(b), (d), (2)(c), (d), (g), (h), (j).

Utility of reporting to the Minister

15.11 AGD doubted it was useful to direct reports on individual warrants and authorisations to the Minister, as compared to oversight agencies. They gave 4 reasons for this.

- The warrant reporting framework under s 49 of the *SD Act* is of 'more limited utility' compared with public annual reporting in providing transparency to the public because such reports are appropriately classified.
- Dedicated ministerial reporting requirements similar to s 49 of the *SD Act* should be 'designed to complement other reporting processes, such as annual reporting on the use of powers and reporting by oversight bodies, and should focus on providing information that may be actionable.'
- '[I]t would not be appropriate for a Minister to intervene in the operational decision making of independent law enforcement agencies based on information contained in reports' and providing the Minister with these reports 'does not enable the Minister to take action.' If there is a concern about noncompliance in an individual case, this is a matter for oversight agencies to address.
- Directing reports to the Minister creates the risk of conflicts of interest and security risks given the sensitivity of information about live, covert investigations.[773]

15.12 In response, the Australian Human Rights Commission and the Ombudsman emphasised that the Minister, unlike the Ombudsman or IGIS, is accountable to Parliament for the operations of AFP and ACIC. Ministerial oversight provides a crucial 'democratic link' necessary to sustain public confidence in the use of extraordinary and covert powers such as *SLAID Act* powers.[774]

> Ministerial reporting is an important accountability measure.

15.13 I recognise that, in practice, oversight agencies are the primary users of reports on individual warrants. However, the provision of these reports to the Minister is consistent with conventions of responsible government and has a broader purpose of demonstrating to the Minister that an appropriate balance is being struck

773 AGD, *Submission 20*, 26.

774 AHRC, *Submission 21*, 13 [44]. Lorraine Finlay, Human Rights Commissioner, *Public hearing transcript*, 19 February 2025, 15. The Ombudsman also said that ministerial reporting is an important accountability mechanism: Ombudsman and INSLM, *Agreed Record of Conversation* (11 February 2025). Also see: Keiran Hardy, Academic Forum, *Public hearing transcript*, 19 February 2025, 65 [15]–[25].

between competing public interests.[775] As stated in the Explanatory Memorandum of the Surveillance Devices Bill 2004 (Cth):

> Importantly, for accountability purposes and in recognition of the balance that must be struck between law enforcement and the right to privacy, the report to the Minister must be provided so that it demonstrates the benefit of the investigation of the use of the SD [surveillance device] and of the use made or to be made or to be of any evidence or information stemming from the use of the SD [surveillance device].[776]

15.14 I also acknowledge that there are limitations (as is appropriate) on the Minister's ability to intervene in decisions about individual operations. However, I do not entirely agree with AGD that the Minister is unable to take any action on the matters contained in individual warrant reports. For example, the Minister can give directions to both AFP[777] and the ACIC Board[778] about the performance of their functions more generally, without interfering with operational matters.[779] The Minister can also ask questions of oversight bodies about any matters of concern. Providing individual warrant reports to the Minister enables the Minister to provide this type of guidance. It also ensures the Minister has awareness of controversial or unusual cases and can seek further information, including from oversight bodies, if required.

775 In our system of responsible government, ministers are accountable to Parliament and, through it, to the community at large: *Australian Capital Television Pty Ltd v Commonwealth* (1992) 177 CLR 106, 184–5 (Dawson J); 135 (Mason CJ).

776 Explanatory Memorandum, Surveillance Devices Bill 2004 (Cth) 41 [257].

777 After obtaining advice from the Commissioner, the Minister may give directions on the general policy to be pursued in the performance of the functions of AFP: *AFP Act* s 37(2).

778 The Minister may give directions or guidelines to ACIC's Board with respect to the performance of its functions: *ACC Act* s 18(1). Functions of ACIC's Board include determining national criminal intelligence priorities; and authorising an intelligence operation to occur: *ACC Act* s 7C(1)(a) and (c).

779 For example, the current direction to AFP contains guidance on the conduct of investigations involving a professional journalist or news media organisation: Hon Mark Dreyfus KC MP, former Attorney-General, *Ministerial Direction to Australian Federal Police* (Cth) (Guideline, 20 October 2023) 3–4.

Who should the Minister share ministerial reports with?

15.15 It is a matter for each individual Minister to determine who should receive reports on their behalf and to set in place arrangements to ensure relevant material is brought to the Minister's attention. The Minister's department and/or relevant oversight bodies may fulfil this 'triaging' function on the Minister's behalf. This type of approach is consistent with normal administrative practice across government. I have not identified any provisions in the *SLAID Act* that would limit the ordinary discretion of a Minister to make administrative arrangements for how reporting to the Minister is to be stored and 'triaged' or summarised for the Minister. If there are any such barriers they should be removed.

> In accordance with normal administrative practice, Ministers can make arrangements for information provided to them to be 'triaged' and summarised.

15.16 It is not in dispute that individual warrant reports should continue to be provided to the relevant oversight body. Indeed, there is an explicit requirement for annual reports to the Minister regarding ATWs and related authorisations to be provided to the Minister and the Ombudsman.[780] IGIS may request copies of reports given to the Minister that relate to ACIC or AFP's performance of their intelligence functions.[781] In my consultations with IGIS and the Ombudsman, both emphasised the benefits of having access to individual warrant reports in exercising their statutory functions.[782]

15.17 I would expect that a newly established Commonwealth PIM (discussed in Chapter 8) would ordinarily rely on the Ombudsman and IGIS reviews and thematic findings of inspections. However, there should be no legislation that prevents ministerial reports from also being shared with the PIM.[783] For example, in some cases the PIM may benefit from being able to review a relevant individual ministerial report to provide accurate advice to the issuing authority about a new warrant dealing with the same subject matter; or an issuing authority may have highlighted a warrant because it is unusual and may require heightened scrutiny.

780 *Crimes Act* s 3ZZVL. A public annual report is also provided for in s 3ZZVM. This is consistent with other warrants in the *Crimes Act* such as the delayed notification search warrant: see *Crimes Act* s 3ZZFB.

781 *Inspector-General of Intelligence and Security Act 1986* (Cth) s 32A(1)(e) (*IGIS Act*).

782 Ombudsman and INSLM, *Agreed Record of Meeting* (11 February 2025); IGIS and INSLM, *Agreed Record of Meeting* (28 February 2025) 3–4.

783 I refer to the role of the NSW SD Commissioner and Qld PIM in maintaining a feedback loop in Chapter 8: *Surveillance Devices Act 2004* (NSW) s 44 and 49; NSW SD Commissioner, *Submission 2*, 19; *Police Powers and Responsibilities Act 2000* (Qld) s 357; Public Interest Monitor (Qld), *Annual Report 2023–2024* (Report, 30 September 2024) 8.

There should be no legislation that prevents oversight bodies or PIMs from having access to warrant reports.

15.18 Any sharing of sensitive information about ongoing covert investigations is a risk, and one that can and should be managed through normal administrative arrangements and existing controls regarding information security.[784] If there is concern that reports are unnecessarily being sent to the department as well as oversight bodies, it is open to the Minister to indicate that they should only go to oversight bodies, which can then draw matters to the Minister's attention as required in the normal course of their inspections.

Normal administrative and policy mechanisms should be applied to properly protect sensitive information.

Scope and content of ministerial reporting

15.19 I am generally satisfied that the list of specified matters that ministerial reports must address is sufficient, though there is scope to improve consistency in certain areas where it will improve effective oversight.

Inconsistencies regarding scope of ministerial reporting

15.20 There are several substantive inconsistencies in reporting requirements across the *SLAID Act* powers. These are summarised in Table 6. Some inconsistencies can be explained by the specific context of a warrant power. For example, because ATWs cannot authorise interception powers, there is no need for reporting in that regard. However, there are some areas where there is no apparent reason for differences in approach between warrants. For example, there is a requirement to report on whether assistance orders have been made for NAWs but no corresponding requirement for DDWs and ATWs.

784 Department of Home Affairs, *Protective Security Policy Framework: Release 2024* (Guideline, 2024). There are also a range of existing offences for improper disclosure by officials, including those in pt 5.6 of the *Criminal Code*.

Table 6 – Inconsistent reporting requirements across the SLAID Act powers

Type of report to Minister	DDW	ATW	NAW
Interception powers were used[785]	✗	N/A	✓
Information obtained was disclosed to others[786]	✗	✓	✓
Information has been destroyed or retained[787]	✗	✗	✓
A computer has been removed[788]	✗	N/A	✓
An assistance order has been made[789]	✗	✗	✓
Details of any concealment activities that have been conducted[790]	✗	✗	✓
Details of any emergency authorisation that has been issued[791]	✓	✗	N/A

15.21 It seems logical that there should be consistent reporting requirements across the *SLAID Act* warrants for each of the matters listed in Table 6, except where the relevant matter does not apply to that type of warrant. Australian Human Rights Commission, Dr Philip Glover and the Internet Association of Australia also argued that these inconsistencies should be addressed.[792]

785 *SD Act* s 49(2E)(xiv) (NAW).
786 *Crimes Act* s 3ZZVL(2)(h)–(i) (ATW); *SD Act* s 49(2E)(ix) (NAW).
787 *SD Act* s 49(2E)(xiii) (NAW).
788 *SD Act* s 49(2E)(xiv) (NAW).
789 *SD Act* s 49(2E)(xvi) (NAW).
790 *SD Act* s 49(2E)(xv) (NAW).
791 *SD Act* s 49(2D)(b)–(e) (DDW). For ATWs, there is only a requirement to report on number of applications, approvals and refusals for emergency authorisations: *Crimes Act* s 3ZZVL(1)(l)–(n). Additional obligations to report on details in *Crimes Act* s 3ZZVL(2), for example, in relation to the benefit and use only apply to executed warrants (and not emergency authorisations).
792 AHRC, *Submission 21*, Recommendation 10; Philip Glover, *Submission 8*, 8; Sophia Joo, IAA, *Public hearing transcript*, 19 February 2025, 39 [25].

15.22 In practice, the Ombudsman and IGIS primarily use these reports, and these agencies are best placed to identify types of information most beneficial to informing their oversight function as well as any information that it is not necessary to report. As such, they should be consulted on any legislative reform.

Recommendation 19: Ministerial reporting requirements should be retained and amended so that:

(a) There are consistent reporting requirements across the *SLAID Act* warrants.

...

15.23 In this recommendation 'consistent' does not mean identical, for example there should be no requirement to report on emergency authorisations for NAWs as such authorisations are not available for NAWs. As indicated above, IGIS and Ombudsman should be consulted on whether all current reporting requirements are necessary and if any have been omitted.

Improving consistency in the nature of information addressed in ministerial reports

15.24 During this review my office examined a significant number of the reports that were provided to the Attorney-General for *SLAID Act* warrants. There was considerable difference in the level of detail provided by the 2 agencies. For example, one of the requirements is to 'give details' of the extent to which the execution of a NAW has assisted the applicant agency in carrying out its functions.[793] Reports from one agency provided meaningful details about how the warrant assisted, while reports from the other agency contained more high-level references to the warrant contributing to the intelligence picture held by the agency.

15.25 Based on my office's review of reports on individual warrants, I consider there is scope to improve the consistency of ministerial reporting. Lack of meaningful detail may not comply with some current statutory requirements and certainly undermines the utility of reports.

15.26 I suggest that the relevant Minister give guidance to AFP and ACIC on the level of detail that should be in the reports. I suggest that this be developed in consultation with IGIS and the Ombudsman. It is a matter for the Minister whether the guidance is administrative in nature or forms part of a general direction made under statute.[794]

Greater guidance is needed on the level of detail to be provided in reports to the Minister.

793 *SD Act* s 49(2E)(viii).
794 *AFP Act* s 37(2); *ACC Act 2002* s 18(1).

Additional requirements for named person account takeover warrants

15.27 In Chapter 6, I recommended the introduction of named person ATWs subject to the introduction of additional safeguards, including additional reporting requirements.

15.28 Additional reporting requirements should be based on existing requirements for named person warrants under the *TIA Act*.[795] For example, reporting on a named person ATW should include information about the accounts that were taken over under the warrant and the reasons it would not have been effective to take over those accounts under a specified account ATW.

> **Recommendation 19: Ministerial reporting requirements should be retained and amended so that:**
>
> **...**
>
> **(b) Reporting on named person ATWs includes details of the accounts that were taken over under the warrant and the reasons it would not have been effective to take over those accounts under a specified account ATW.**
>
> **...**

15.29 Consultation should be undertaken with the relevant oversight agencies on any other appropriate reporting requirements before expanding ATWs.

Timeliness of ministerial reporting

15.30 For DDWs and NAWs, the requirement to report 'as soon as practicable' to the Minister is only enlivened after the warrant or authority 'ceases to be in force.'[796] As I have explained in Chapter 6, the absence of any current limit on the number of times a 90-day NAW can be renewed is problematic because the requirement to report is not triggered until the warrant ceases to have effect. Therefore, there may be an 'extended period of time in which the Minister is not being provided any

795 *TIA Act* s 94B(3).

796 *SD Act* s 49. The requirement to report 'as soon as practicable' is different from some other warrant reporting requirements, which require a report to be provided within a set number of days. See *TIA Act* s 17 and sch 1, cl 130. In both of these examples, a report is required to be provided to the Attorney-General within 3 months. IGIS has noted this difference: IGIS, Submission No 18 to PJCIS, Parliament of Australia, *Review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (26 February 2021) 10 [38].

substantive information about the execution of the warrant.'[797] In practice, these reports form an important part of the oversight process and can be the trigger for an inspection. It is not sufficient for the Minister or oversight agencies to have to request and rely on what information the agency chooses to put in an affidavit associated with seeking an extension.

> Currently, there is a risk that there will be long gaps in ministerial reporting for NAWs because the requirement to report is not triggered until the warrant ceases to have effect.

15.31 In Chapter 6, I have recommended extending the maximum duration of NAWs to 6 months. As I said in that chapter, my preferred mechanism for achieving this would be to make NAWs non-renewable. This would ensure that there is a trigger for reporting at the end of 6 months. In the alternative, there should be legislative amendment to ensure that, at a minimum, ministerial reporting occurs every 6 months.

15.32 The issue of timely reporting has not arisen in practice with DDWs. The *SD Act* permits multiple extensions of DDWs, but in practice this has not occurred.[798] Regardless, for reasons analogous to those discussed in relation to NAWs, there should be legislative amendment to ensure there is an obligation to report to the Minister at least every 6 months if any DDWs are renewed multiple times.[799]

15.33 As discussed earlier in this chapter, reporting on ATWs is currently annual. I acknowledge that the Ombudsman said that, because of the 'relatively low use' of ATWs compared with other powers, annual reporting 'is sufficient to enable appropriate oversight.'[800] However, annual reporting still leaves a potentially wide temporal gap between when warrants are executed and when reports are provided to the Minister. Accordingly, I consider that the *Crimes Act* should be amended to ensure that there are reporting requirements for each ATW, like other *SLAID Act* warrants.[801] As with NAWs and DDWs, where an ATW has effect for longer than 6 months (due to extensions), ministerial reporting should be required at least every 6 months.

797 IGIS, *Submission 9*, 5 [20]. This has been the case in practice, given that the majority of NAWs have been extended at least once and some multiple times.
798 *SD Act* s 27KF(1)(a).
799 Note also Chapter 6 about the ability to extend these warrants.
800 Ombudsman, *Submission 11*, 5.
801 See also Chapter 6 about the ability to extend these warrants.

Timeframe for production of reports

15.34 It is also necessary to consider the timeframe in which agencies are required to produce a ministerial report once an obligation to do so has arisen. IGIS considered that there may be benefit in establishing a more definite timeframe for reporting at the conclusion of the warrant or when they are renewed.[802] AGD agreed that, if regular mandatory reporting to the Minister was retained, 'there would be value in providing a fixed timeframe for the provision of warrant reports.'[803]

15.35 Currently, reports are to be provided 'as soon as practicable' after the reporting date. I considered whether this should be amended to a specific timeframe, as is the case with some other types of warrants.[804] If a short timeframe is set, there is a risk that quality reports on particularly complex matters may not be able to be provided in a short time. If a longer timeframe is set, there is a risk that reports will be delayed to the maximum time rather than being provided sooner where possible. There were no submissions raising concerns that the requirement to provide reports 'as soon as practicable' had resulted in reports not being provided within a reasonable time. Should an issue arise as to the timeliness of reports, this is something that IGIS and the Ombudsman could provide guidance and public reporting on. There is also the option of ministers giving guidance. With these factors in mind, I see no reason to set a fixed statutory maximum time for reports to be provided. If, contrary to this view, a timeframe is preferred then it should be expressed as 'as soon as practicable and no later than 3 months.'

802 IGIS, *Submission 9*, 5 [21].
803 AGD, *Supplementary response and submission 28*, 5.
804 For example, reports on law enforcement telecommunications interception warrants must be provided within 3 months: *TIA Act* s 94(2). AGD said that, if regular mandatory reporting to the Minister is retained, 'there would be value in providing a fixed timeframe for the provision of warrant reports' consistent with the 3 months timeframe for reporting in the *TIA Act*: AGD, *Supplementary submission 28*, 5.

Recommendation on ministerial reporting

Recommendation 19: Ministerial reporting requirements should be retained and amended so that:

(a) There are consistent reporting requirements across the *SLAID Act* warrants.

(b) Reporting on named person ATWs includes details of the accounts that were taken over under the warrant and the reasons it would not have been effective to take over those accounts under a specified account ATW.

(c) There is no more than 6 months between the warrant being issued and the requirement to provide a report to the Minister being triggered.

(d) Individual reports on ATWs are required.

Public reporting

15.36 Public reporting on the use of covert powers plays an important role in 'promoting transparency around, and building and sustaining public confidence in, the use of such powers.'[805] This is achieved by providing accurate and accessible information about how frequently (or infrequently) different powers are used, what they are used for and the operation and outcomes of scrutiny and safeguard mechanisms.

15.37 Public reporting is also part of parliamentary scrutiny, as the annual reports tabled in Parliament are the main source of information for the Parliament about the use and utility of the powers they have enacted.

15.38 As discussed in Chapter 4, the current reporting is of little value in providing evidence of the utility of *SLAID Act* warrants. The main measure (arrests and prosecutions) has little relevance to *SLAID Act* warrants because NAWs cannot be used as evidence, DDWs are intended for circumstances were a prosecution is not feasible and ATWs are an authority to take over an account, after which different powers are used to collect evidence from the account.

15.39 There are 2 ways to improve what is currently publicly reported: first, by providing more statistical reporting; and, second, by publishing an annual statement describing how the powers that were used have assisted in the investigation, disruption and prevention of serious crime. Not all information about the use of *SLAID Act* powers can be published without prejudice to ongoing law enforcement and intelligence operations or other harms, and there needs to be a clear mechanism to determine when public reporting should be delayed.

805 AGD, *Supplementary submission 28*, 1.

Current requirements for annual public reporting

15.40 Annual reports for DDWs, NAWs and ATWs must include, among other matters, the following statistical information:[806]

- the number of applications for warrants and the number of warrants issued or extended[807]
- the number of arrests made during that year 'on the basis (wholly or partly) of information obtained' under a DDW, NAW or ATW and the number of resulting prosecutions[808]
- the number of applications for emergency authorisations (not applicable to NAWs).[809]

15.41 For DDWs and NAWs, there is provision for the Minister to specify additional information for reporting that the Minister considers appropriate.[810]

15.42 The reports must also describe (at a high level) the types of offences the warrants were sought for.[811] This information is useful in providing an indication of the types of offences the powers are being directed to. It should be retained.

Additional public reporting is required

15.43 Existing statistical reporting on the number of applications for warrants, the number of warrants issued or extended and the number of applications for emergency authorisations is useful and should be retained. Statistics on the number of arrests and prosecutions are of limited utility but could be retained, or could be incorporated in the proposed qualitative reporting about how the powers have assisted in the investigation, disruption and prevention of serious crime

Reports could include more statistics

15.44 Statistical reporting is not a complete answer to increasing the amount of information about the utility of warrants that is communicated. But it can go some way toward increasing transparency and reducing some concerns by also demonstrating the ways warrants are *not* used. Additional statistical reporting could also shed more light on the process for scrutinising applications.

806 Information is provided to the Minister, who must table a report within 15 sitting days of receiving it.
807 *SD Act* s 50(1)(a), (f); *Crimes Act* s 3ZZVM(1)(a), (b), (g).
808 *SD Act* s 50(1)(g), (i); *Crimes Act* s 3ZZVM(1)(p), (q).
809 *SD Act* s 50(1)(b); *Crimes Act* s 3ZZVM(1)(i).
810 *SD Act* s 50(1)(j). Based on the information contained in public reports, this provision does not appear to have been utilised. There is not a similar power under the *Crimes Act* for ATW annual reports.
811 *SD Act* s 50(1)(eb) and (ec), *Crimes Act* s 3ZZVM(1)(o).

15.45 I note AGD's comments that, if I recommend that warrants have a fixed maximum period – for example, that NAWs be 6 months but not subject to renewal – this may lead to reports giving an inaccurate perception of how many warrants are being issued.[812] I think this comment is suggesting that reporting one warrant has been renewed 5 times would be less concerning to the public than 6 warrants being issued. If that is AGD's view, there is no reason that statistical reporting cannot be accompanied by commentary to explain how many warrants have effectively been 'reissued' for the same operation. Indeed, this would be beneficial.

Sensitive categories of information

15.46 As explained in Chapter 11, some stakeholders expressed doubt about the extent to which the current legislative framework protects special categories of information. In particular, there was concern that *SLAID Act* warrants were being used to target journalists.[813]

15.47 It appears that this concern is in part the result of the limited publicly available information. For example, the Alliance for Journalists' Freedoms said that 'given the lack of data around the use of [*SLAID Act* warrants], it is difficult to know if the current disclosure and secondary disclosure provisions are appropriate.'[814]

15.48 I was pleased that, in this review, AFP and ACIC took the opportunity to make clear that *SLAID Act* powers have not been used to target journalists or media organisations.[815]

15.49 In other Five Eyes jurisdictions there are requirements to include information in annual reports about circumstances where a warrant involved sensitive categories of information.[816] For example, in the United Kingdom, IPCO annual reports include:

- the number of targeted equipment interference warrants involving confidential material (including where LPP information is sought or collaterally could be obtained; and warrants involving sensitive professions such as medical doctor, lawyer, journalist, member of legislature and minister of religion)[817]

812 AGD, *Supplementary submission 28*, 5–6.

813 AJF, *Submission 7*, 1–2 [1.2]–[2.2]; AHRC, *Submission 21*, 11–12 [37]–[39]. The Joint Academic Submission expressed concern about 'the potential to inappropriately burden press freedom' arising from broadly expressed *SLAID Act* powers and wide secrecy and espionage offences: Joint Academic Submission, *Submission 15*, 10. See generally Rebecca Ananian-Welsh, Sarah Kendall and Richard Murray, 'Risk and Uncertainty in Public Interest Journalism: The Impact of Espionage Law on Press Freedom' (2021) 44(3) *Melbourne University Law Review* 764.

814 AJF, *Submission 7*, 6 [5.4].

815 Ian McCartney, Deputy Commissioner, AFP, *Public hearing transcript*, 20 February 2025, 23 [15]. Email from ACIC to INSLM, 11 July 2025.

816 *Investigatory Powers Act 2016* (UK) s 234(2)(c) (LPP information, confidential journalistic material and sources of journalistic information).

817 In 2023 in the United Kingdom (UK), there were 12 targeted equipment interference warrants where LPP information was sought, 213 where LPP information might possibly be obtained and 88 involving sensitive professions: Investigatory Powers Commissioner's Office, *Annual Report 2023* (Report, 22 May 2025) 94.

- for applications for communications data, a further breakdown of the proportion of warrants relating to particular sensitive professions
- the number of applications made for warrants where the purpose was to obtain material which the applicant authority believed would relate to confidential journalistic material. [818]

15.50 There is scope for similar statistical reporting in Australia.

15.51 AGD suggested that any new reporting requirement regarding journalists should be for journalists acting in their *professional capacity* rather than for a person who happens to be a journalist but is also involved in unrelated criminal activity.[819] I suggest that the focus be on whether a protected category of *information* is likely to be obtained, as it is this information, rather than a profession, that requires protection. For example, an investigation of a lawyer who is suspected of money laundering would not be an investigation into action undertaken in the lawyer's *professional capacity* (money laundering not being a lawful activity or consistent with legal professional obligations). Nevertheless, if the use of special powers is likely to result in the collection of privileged information, that should be reported.

Recommendation 20: Public annual reporting requirements should be amended to include:

(a) The number of warrants where specified categories of sensitive information is sought or is likely to be obtained (including LPP and journalist source information).

...

15.52 It should also be open to the Minister to include contextual information in a report where appropriate (for example, that any legal professional privilege material that was collected was quarantined and not able to be accessed by investigators). The NSW SD Commissioner observed that in New South Wales contextual information had been included in public annual reporting on use of surveillance devices through a provision allowing for reporting on 'any other information relating to the use of surveillance devices and the administration of the [Surveillance Devices Act 2007 (NSW)] that the Attorney General considers appropriate.'[820] This was used in the 2023–24 reporting period as the basis for providing information considered

818 Investigatory Powers Commissioner's Office, *Annual Report 2023* (Report, 22 May 2025) 95; 20 [4.12].
819 AGD, *Supplementary submission 28,* 3.
820 NSW SD Commissioner, *Supplementary submission 25*, 4; *Surveillance Devices Act 2007* (NSW) s 45(1)(c).

'appropriate to provide a more comprehensive representation of the manner in which the Act is being administered.'[821]

Number of people subject to surveillance, account takeover or disruption

15.53 A single *SLAID Act* warrant can affect many individuals. This is especially true for NAWs, but it also applies to ATWs and DDWs. In 2019, the Comprehensive Review said that there was scope to introduce new reporting requirements to provide the Parliament and the public with more meaningful information about the use of electronic surveillance powers. One of the categories suggested in that report was '[t]he number of people who have been the subject of electronic surveillance, in addition to the number of warrants and authorisations issued – to ensure that the report provides more meaningful information about the extent of the use of surveillance powers.'[822]

15.54 I support this principle. I also recognise that in some instances only an estimate will be able to be provided, especially for NAWs, because it may not (or not yet) be possible to determine whether various 'identifiers' collected relate to different individuals. An alternative for NAWs would be to require reporting on the number of individuals who were *identifiable* in the information collected. For DDWs it may be more appropriate to report on the number of devices disrupted and for ATWs the number of accounts taken over during the year. This information should already be being collected for ministerial reporting and oversight purposes.

Recommendation 20: Public annual reporting requirements should be amended to include:

...

(b) The number of people, devices and accounts affected by each category of warrant (NAW, DDW and ATW).

...

821 NSW SD Commissioner, *Supplementary submission 25*, 5; Attorney General (NSW), *Report by the Attorney General of New South Wales Pursuant to Section 45 of the Surveillance Devices Act 2007 for the Period Ended 30 June 2024* (Report, 10 January 2025) 4–6.

822 *2019 Comprehensive Review*, vol 2, 440 [31.43].

Scrutiny of applications

15.55 Currently, AFP and ACIC must report on the number of applications for warrants, emergency authorisations and extensions that were refused during that year.[823]

15.56 The 2019 Comprehensive Review Report identified:

> [There is scope for additional public reporting on the process of scrutinising applications, such as] the number of occasions on which issuing authorities have required agencies to provide further information in support of warrant applications, or issued a warrant in terms other than those initially sought by the agency, in addition to the number of warrants issued and refused – to ensure that the report more accurately reflects the role that issuing authorities play in scrutinising applications.[824]

15.57 I agree that it would be beneficial for public reporting to include information about the number of occasions on which agencies were required to provide further information in support of warrant applications; or issued a warrant in terms other than those the agency initially sought. This occurs in other jurisdictions. For instance, IPCO annual reports include reporting about the number of applications returned for further detail and the reasons these applications are returned to applicants.[825]

15.58 For NAWs and DDWs, there is also a requirement to report on the reasons for a refusal. This should be extended to ATWs. Reasons for refusal of any warrant should include a sufficient level of detail to make the reasons understandable.

15.59 Canada provides perhaps the 'high watermark' for publishing details on why a warrant has been refused.[826] Canada's system is different and it is not suggested that the level of detail that is published for Canadian intelligence warrants is needed for *SLAID Act* or other law enforcement warrants in Australia. However, the level of detail that can be provided publicly in Canada without prejudice to national security or operations indicates that there is considerable scope for more detail to be made publicly available than is currently the case in Australia. A more detailed (not necessarily public) set of reasons for refusal or imposition of conditions would be a useful resource for applicants and PIMs and a way to develop some (non-binding) guidance for issuing authorities in order to increase consistency in warrant issuing.

---

823 *SD Act* s 50(1)(e) and in relation to extensions sought but refused: s 50(1)(f). *Crimes Act* s 3ZZVM(1)(c), 3ZZVM(1)(f), 3ZZVM(1)(h), 3ZZVM(1)(k), (n).

824 *2019 Comprehensive Review*, vol 2, 440 [31.43].

825 Investigatory Powers Commissioner's Office (UK), *Annual Report of the Investigatory Powers Commissioner 2023* (22 May 2025) 99–100, Table 14.8 and Table 14.9.

826 Reason are published on 'Decisions,' *Office of the Intelligence Commissioner (Canada)* (Web Page, 13 June 2025). See, for example, Intelligence Commissioner (Canada), *Decision 2200-A-2023-07 In relation to the determination of a class of acts or omissions that would otherwise constitute offences pursuant to subsection 20.1(3) of the Canadian Security Intelligence Service Act and Section 19 of the Intelligence Commissioner Act* (21 June 2023).

15.60 In view of other findings and recommendations in this report about the system for issuing warrants, some additional reporting is appropriate, including:

- the number of warrants granted with conditions and, at a high level, the nature of the condition (for example, where a condition is imposed to minimise the risk of incidentally collecting LPP information). Reporting should identify whether the number (or percentage) of conditions that were mandatory statutory conditions (if applicable), proposed in the application or imposed by the issuing authority
  - scrutiny by PIMs, including the number of draft warrants that they provided 'comment' on and the number that they provided submissions on (see Chapter 8)
  - the work of the technical advisors, including (at a high level) the general guidance they provide (similar to IPCO) and the number of individual warrant applications they are called to give specific advice on.

Recommendation 20: Public annual reporting requirements should be amended to include:

...

(c) Reasons for refusal of an ATW (consistent with the existing requirement for DDWs and NAWs).

(d) The number of occasions on which issuing authorities have required agencies to provide further information in support of warrant applications; the number of warrants granted with conditions; input of Commonwealth PIMs in warrant issuing; and, the work of the technical advisors.

...

15.61 As discussed in Chapter 9, some of this data should be collated by the secretariat supporting dedicated Commonwealth issuing authorities rather than agencies.

Assistance orders

15.62 AFP and ACIC are not currently required to publicly report on the utilisation of assistance orders. In their submissions to the PJCIS, and to this review, the Ombudsman, the Law Council of Australia and the Australian Human Rights Commission recommended that agencies be required to keep records of, and publicly report on, this information, on the basis that it would increase transparency and accountability.[827]

827 Ombudsman, *Submission 11,* 6; Law Council, *Submission 23,* 71 [269]; Ombudsman, Submission No 5 to the PJCIS, Parliament of Australia, *Review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (February 2021) 4; Law Council, Submission No 21 to the PJCIS, Parliament of Australia, *Review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (9 March 2021) 112–113 [398]–[402]; AHRC, *Submission 21,* Recommendation 11.

15.63 AGD initially suggested that 'reporting the number of assistance orders may provide limited utility as these orders are facilitative and operate solely to assist the execution of a [*SLAID Act* warrant].'[828] It said that 'extensive reporting' on the warrants to which assistance orders would be attached provides for sufficient public oversight and accountability. It later clarified that it 'does not have any concerns about additional reporting on the number of assistance orders' in general; however, in particular cases, it could 'enable inferences to be drawn about who may have provided assistance.'[829]

15.64 I do not agree that the current public reporting on *SLAID Act* warrants can be described as 'extensive reporting' or that reporting on the number of times an extraordinary power has been used is of 'limited utility.' As discussed in Chapter 14, assistance orders can compel cooperation from a range of people, including those not suspected of any wrongdoing. There was considerable concern, including from industry groups, about how these powers might be being used.

15.65 In the first 3 years of the operation of the *SLAID Act* there were in fact no assistance orders sought.[830] This information was provided to this review by AFP and ACIC – they did not seek to argue that disclosing that no assistance orders had been sought would reveal operationally sensitive information. Public acknowledgment that no, or very few, assistance orders have been sought provides assurance that this extraordinary power is not being overused.

15.66 The number of assistance orders sought, granted and used each year should be routinely included in public annual reporting. On rare occasions it may be necessary to delay reporting if it could prejudice an operation or cause other harm (see discussion below).

Recommendation 20: Public annual reporting requirements should be amended to include:

…

(e) The number of assistance orders sought, granted and used each year.

…

828 AGD, *Submission 20*, 27.
829 AGD, *Supplementary submission 28*, 2.
830 The exact period for which information on warrants was sought during this review was from the commencement of the powers to 31 December 2024. In that period no assistance orders were sought.

Reports could do more to describe effectiveness

15.67 Multiple civil society groups highlighted the limited publicly available evidence base supporting the effectiveness of *SLAID Act* powers.[831] For example, the Internet Association of Australia said that:

> Given the extremely invasive nature of the SLAID powers, we believe there should be more information on where these powers have been deemed to be not only necessary in the investigation of serious crimes but also the only or best measure available to the AFP and/or ACIC in addressing such crimes.[832]

15.68 Statistical information is valuable. However, particularly for warrants that are for an intelligence purpose or are not intended to lead directly to prosecutions, it cannot provide a qualitative picture of the utility of the warrants.

15.69 AGD agreed that 'the provision of qualitative information may assist with public understanding of the *SLAID Act* powers, and may also assist in building and sustaining confidence in the framework.' However, AGD also noted it may be difficult to describe the benefits of long-term intelligence operations in a particular year.[833]

15.70 I recognise that it is difficult to measure and attribute a successful outcome to the use of a specific power, particularly in the types of complex investigations in which *SLAID Act* powers are likely to be used. In response to a request for information about what additional material could be provided to illustrate the effectiveness of the *SLAID Act* powers, AFP noted the difficulties in measuring their effectiveness:

> Measuring success in a policing agency is complex. Arrests and prosecutions are not the only measures of success. From the AFP's perspective, prevention and disruption of crime are successful outcomes, however, can be difficult to measure. Furthermore, the investigations where AFP uses SLAID powers are typically complex, protracted and criminality can significantly vary.[834]

15.71 When asked about how they measure 'success' of warrants internally, ACIC said one measure is the number of intelligence products they are generating:

> One measure of our own success might be, although quite linear, the number of products that we're actually generating off network activity warrants, which is quite significant.[835]

15.72 Based on the information published during this review, including in the public hearing and in the agreed unclassified summaries of private hearings, I consider that there is clearly scope to increase the amount of material made publicly available that describes the effectiveness of the *SLAID Act* powers. Public confidence will be increased if law enforcement and criminal intelligence agencies seek to communicate as clearly as possible how special powers are used and why they are effective in detecting and disrupting serious crime.

831 QCCL, *Submission 6*, 7; HRLC, *Submission 5*, 11; Philip Glover, *Submission 8*, 2–3; Law Council, *Submission 23*, 24–28.
832 IAA, *Submission 16*, 1.
833 AGD, *Supplementary submission 28*, 3.
834 AFP, *Supplementary submission 29*, 1.
835 Matthew Rippon, Deputy CEO, ACIC, *Public hearing transcript*, 20 February 2025, 45 [5].

15.73 The legislation should require that annual reporting provide a statement as to how the use of particular types of *SLAID Act* warrants (for example, NAWs) have enhanced the agency's ability to investigate, disrupt and prosecute (as relevant) serious crime. As far as possible, this should include why other powers were likely to be ineffective in the circumstances. The expectation should be that every effort is made to describe the use of the powers in the relevant year as effectively as possible, without compromising operations or capabilities. The kind of qualitative information that can be provided will depend on the agency and how they are using the warrants. Where applicable, multi-year operations may need to be reported on multiple times or only after completion.

Recommendation 20: Public annual reporting requirements should be amended to include:

...

(f) An annual statement that describes, as far as possible, how the use of each type of warrant has enhanced the ability of each agency to investigate, disrupt and prosecute (as relevant) serious crime.

...

Secrecy provisions should not prevent agencies publishing additional information about utility

15.74 Separate from formal public reporting, AFP and ACIC often communicate successful law enforcement outcomes to the public through the media.[836] AFP suggested that, for *SLAID Act* warrants, it might be able to publicly disclose 'high-level case studies at a time and level of detail that AFP assesses would not compromise ongoing investigations or operational sensitivities' but that it is currently prevented from making these disclosures by the overly restrictive secrecy provisions.[837]

15.75 As discussed in Chapter 12, the secrecy provisions should be amended for a range of reasons. Amongst other things, the proposed amendments will allow agencies to use their discretion to report outcomes. This kind of publicity does not remove or reduce the need for mandatory annual public reporting to be as meaningful and objective as is possible.

836 For example, AFP, 'AFP Takes the Fight to Cybercriminals in 2024' (Media Release, 30 December 2024); ACIC, 'Alleged QLD Money Laundering Organisation Dismantled after Washing More than $10 million, Four Charged' (Media Release, 9 June 2025).Referencing these operations in this context does not imply that *SLAID Act* warrants were used in these operations.

837 AFP, *Supplementary submission 29*, 1.

There will always be some information that cannot be reported

15.76 There will always be some information that cannot be publicly reported, or cannot be reported at that time, without genuine risk of compromising current operations or covert technical capabilities. Legislation should clearly set out reasons why information may be withheld.

15.77 There is an existing mechanism in s 50A of the *SD Act* that concerns surveillance powers used in relation to a limited class of persons. As noted by AGD, this may provide a model for setting out when information should not be included in a particular annual report.[838] It should apply to circumstances where disclosure would be likely to prejudice an operation or prosecution or reveal the identity of a person who has assisted with the execution of a warrant, including under an assistance order where there is a risk that such a disclosure could lead to some form of harm.

Recommendation 20: Public annual reporting requirements should be amended to include:

...

(g) A framework for deferred reporting based on that in s 50A of the *SD Act*.

Additional reporting opportunities may be identified

15.78 Beyond the parameters canvassed in this chapter, there may be scope for additional reporting with a focus on *SLAID Act* warrants. I welcome AGD's acknowledgement that 'there may be scope to strengthen reporting requirements to provide the Parliament and public with more meaningful information' and acknowledge its view that this should be pursued in the context of broader electronic surveillance reform.[839]

15.79 AGD also noted the additional parameters for reporting suggested by the 2019 Comprehensive Review. Those parameters included the use of electronic surveillance information in the hearings and reports of integrity agencies; and reporting on outcomes in matters in which electronic surveillance was used as part of an investigation (but not given in evidence) – for example, where an accused person may have entered a plea of guilty on the strength of the case against them (but electronic surveillance material was not adduced in evidence). It is not immediately clear that these are directly relevant to *SLAID Act* warrants given the definition of 'relevant offence' and limitations on use in evidence. However, I agree with the goal of providing any additional information that may assist 'to provide a

838 AGD, *Supplementary submission 28*, 2.
839 AGD, *Supplementary submission 28*, 1.

more complete picture of the purposes for which surveillance information may be used.'[840]

Recommendation on public reporting

There is scope to improve current public reporting mechanisms. In addition to current statistical reporting on the number of warrants (etc) the following additional information should be reported, subject to rare cases where there may need to be deferred reporting.

Recommendation 20: Public annual reporting requirements should be amended to include:

(a) The number of warrants where specified categories of sensitive information is sought or is likely to be obtained (including LPP and journalist source information).

(b) The number of people, devices and accounts affected by each category of warrant (NAW, DDW and ATW).

(c) Reasons for refusal of an ATW (consistent with the existing requirement for DDWs and NAWs).

(d) The number of occasions on which issuing authorities have required agencies to provide further information in support of warrant applications; the number of warrants granted with conditions; input of Commonwealth PIMs in warrant issuing; and, the work of the technical advisors.

(e) The number of assistance orders sought, granted and used each year.

(f) An annual statement that describes, as far as possible, how the use of each type of warrant has enhanced the ability of each agency to investigate, disrupt and prosecute (as relevant) serious crime.

(g) A framework for deferred reporting based on that in s 50A of the *SD Act*.

840 AGD, *Supplementary submission 28*, 2.

Chapter 16: Oversight

16.1 Robust and credible oversight is essential to public trust in the work of law enforcement and criminal intelligence agencies. Because of the inherently covert nature of *SLAID Act* powers, there are limited opportunities for affected individuals to seek review through traditional mechanisms such as the courts. There is also some information about the way these powers are used and the capabilities that underpin them which cannot be made public without prejudice to the effectiveness of the powers. In this context, it is critical that there be robust independent oversight.

16.2 Previous reviews have proposed different ways of dividing oversight of AFP and ACIC between the Ombudsman and IGIS. That question is broader than *SLAID Act* powers alone. Assessing the most effective overall scheme and division of responsibility for oversight of covert powers was beyond the scope of this review.

16.3 Instead, this chapter focuses on changes that should be made to enhance oversight arrangements for *SLAID Act* powers, regardless of possible future changes to the exact boundary between IGIS and Ombudsman oversight of AFP and ACIC. Five main changes are recommended in this chapter:

- There should be no legislative barriers to information sharing between oversight agencies.
- Oversight agencies should be able to access the proposed technical advisory panel.
- The Ombudsman should not be constrained by unnecessarily prescriptive inspection requirements.
- There is opportunity to make record keeping and notification requirements more flexible by replacing detailed (and inconsistent) statutory requirements with a scheme that allows for binding administrative guidance.
- IGIS and the Ombudsman should be able to brief parliamentary committees and IGIS should be able to publish unclassified reports about SLAID Act inspections and inquiries at any time.

Division of oversight responsibility for SLAID Act powers

16.4 To understand the current oversight scheme, it is necessary to briefly outline the current arrangement, including differences between IGIS and Ombudsman oversight. For context, it is useful to also be aware of recent proposals to shift responsibility for oversight of some (or all) AFP and ACIC activities between the Ombudsman and IGIS.

Current arrangements

16.5 Currently, the Ombudsman and IGIS oversee different aspects of AFP's and ACIC's use of *SLAID Act* powers. The scope of inspections by the Ombudsman and IGIS and how they report on oversight activities also differs.

16.6 The Ombudsman performs a broad range of review, inspection and complaint resolution functions under the *Ombudsman Act 1976* (Cth)[841] as well as several other Acts.[842] Ombudsman functions stretch across almost all Commonwealth agencies, as well as some industry matters.[843] The *SLAID Act* extended the Ombudsman's inspection role to DDWs and ATWs, but not NAWs. [844] This was said to be consistent with the oversight responsibility of the Ombudsman regarding other law enforcement powers in the *SD Act*.[845] The Ombudsman also has oversight responsibility for other law enforcement powers under the *SD Act*, *Crimes Act*, *TIA Act* and *Telecommunications Act 1997* (Cth).

16.7 IGIS provides oversight of the activities of Australia's 6 main intelligence agencies: (ASIO, Australian Secret Intelligence Service, ASD, Australian Geospatial-Intelligence Organisation, Defence Intelligence Organisation and Office of National Intelligence. These 6 agencies are exempt from most other forms of oversight, including freedom of information and the jurisdiction of the Privacy Commissioner, the Ombudsman and the Australian Human Rights Commission.[846] Opportunities for review of the actions of these agencies by the ART or courts is very limited.[847] To provide for IGIS oversight of NAWs, the *Inspector-General of Intelligence and Security Act 1986* (Cth) (*IGIS Act*) was amended to expand IGIS's jurisdiction to cover matters related to the 'intelligence functions' of ACIC and AFP. 'Intelligence functions' was defined in such a way that, effectively, IGIS oversight of AFP and ACIC is limited to the use of NAWs and does not encompass the broader intelligence functions of either agency.[848] The reason for conferring oversight responsibility for NAWs on IGIS was to do with the nature of the NAW as an intelligence collection tool.[849]

16.8 In general, legislation about the timing and nature of the Ombudsman's inspection of law enforcement use of warrants is quite prescriptive in comparison to the

841 See *Ombudsman Act 1976* (Cth) s 5.

842 These include *AFP Act* and *TIA Act*. The Ombudsman is also vested with a range of industry oversight functions, such as *Ombudsman Act* pt IID (Private Health Insurance Ombudsman); pt IIE (VET Student Loans Ombudsman); and pt IIF (National Student Ombudsman).

843 See *Ombudsman Act* ss 5(2)(e), 19ZJ, 20D and 20ZM.

844 *SD Act* s 55(1) (DDWs); *Crimes Act* s 3ZZVR (ATWs).

845 Revised Explanatory Memorandum, 4 [13].

846 *Freedom of Information Act 1982* (Cth) s 7(2A)–(2D); *Privacy Act 1988* (Cth) ss 7(1)(f)–(g), (h); *Ombudsman Act* s 5(2)(e); *Australian Human Rights Commission Act 1986* (Cth) s 11(3), (4).

847 *ASIO Act* pt IV and pt IVA; *Administrative Decisions (Judicial Review) Act 1977* (Cth) s 3, sch 1(d); Jake Blight, 'Powers and Functions of National Security Agencies' in Danielle Ireland-Piper (ed), *National Security Law in Australia* (The Federation Press, 2024) 39, 40.

848 *IGIS Act* s 3 (definition of 'intelligence function').

849 Revised Explanatory Memorandum, 5 [24].

jurisdiction of IGIS.[850] In overseeing the use of both ATWs and DDWs, the Ombudsman is *required* to 'inspect the records' of AFP or ACIC to 'determine the extent of compliance' with the legislation by the agency or officers of the agency.[851] The Ombudsman must conduct inspections of ATWs at least once every 12 months.[852]

16.9 In addition to this inspection function, the Ombudsman has its general function for departments and prescribed authorities (including AFP and ACIC) to undertake formal 'investigations' into matters of administration.[853] Following an investigation, where the Ombudsman is of the opinion that a decision was contrary to law, unreasonable, unjust, oppressive or improperly discriminatory or otherwise wrong in all the circumstances, they may recommend that some particular action could be, and should be, taken to rectify, mitigate or alter the effects of a decision.[854]

16.10 In contrast, IGIS has a broader and more flexible inspection function in relation to NAWs. Rather than being set out as legislative requirements, IGIS decides on the timing and scope of inspections, in consultation with the head of the relevant agency.[855] The potential scope of IGIS inspections is broad and can go to not only compliance with the law but also the effectiveness and appropriateness of the procedures and matters relating to the 'propriety' of the activities of agencies.[856] IGIS also has broadly defined inquiry functions that include legality, propriety and consistency with human rights.[857]

Oversight responsibility for *SLAID Act* powers is currently divided between IGIS and the Ombudsman. IGIS has a broader and more flexible remit for inspections.

850 The *2019 Comprehensive Review* recommended against retaining a prescriptive approach to the Ombudsman inspections of electronic surveillance powers, noting that a 'prescriptive approach … risks missing broader compliance and systemic issues': *2019 Comprehensive Review,* vol 2, 434 [31.22].

851 *Crimes Act* s 3ZZVR (ATWs); *SD Act* s 55(1) (DDWs).

852 *Crimes Act* s 3ZZVR (ATWs).

853 *Ombudsman Act* s 5, 7A, 8. AFP) and ACIC) are 'prescribed authorities': *see Ombudsman Act* s 3(a); *Ombudsman Regulations 2017* (Cth) r 8.

854 *Ombudsman Act* s 15(2)(b). Civil Liberties Australia emphasised that the Ombudsman 'has no power to adjudicate': Civil Liberties Australia, *Submission 4*, 1.

855 *IGIS Act* s 9A(1).

856 *IGIS Act* s 4(a)(ii), 9A.

857 *IGIS Act* s 8(3A) (Intelligence agency inquiry functions in relation to ACIC or the Australian Federal Police).

Recent proposals for change to division of oversight responsibilities

16.11 There have been different proposals and actions in recent years to change the division of oversight responsibilities in relation to ACIC and AFP between IGIS and the Ombudsman. Briefly, the main ones were as follows.

- The 2017 Independent Intelligence Review recommended that oversight of all of the National Intelligence Community, including the 'intelligence functions' of AFP and ACIC, be transferred from the Ombudsman to IGIS.[858]
- The 2019 Comprehensive Review Report said that IGIS should not have oversight of AFP but that there was a 'stronger case' for IGIS to have oversight of ACIC. In relation to electronic surveillance, the 2019 Comprehensive Review suggested consolidating all oversight functions for all agencies (including state and territory agencies) using electronic surveillance powers (other than ASIO) with the Ombudsman.[859] This would presumably include all ACIC use of electronic surveillance.
- In 2021, the *SLAID Act* gave oversight of AFP and ACIC use of NAWs to IGIS and gave AFP and ACIC use of ATWs and DDWs to the Ombudsman.
- The Intelligence Services Legislation Amendment Bill 2023 (Cth) (ISLAB Bill) sought to transfer oversight responsibility for ACIC in its entirety, and oversight of the 'intelligence functions' of AFP, to IGIS. The ISLAB Bill lapsed with the prorogation of Parliament in March 2025.[860]
- The ACIC Review recommended that ACIC should be oversighted by IGIS, rather than the Ombudsman.[861]

858 Department of the Prime Minister and Cabinet (Cth), *2017 Independent Intelligence Review* (Report, June 2017) Recommendation 15.

859 *2019 Comprehensive Review*, vol 3, 262, Recommendation 168 (consolidating oversight functions in CO); vol 2, 433, Recommendation 129. This recommendation was also accepted by government: Government response to the Comprehensive Review, 36–7. AGD added that '[t]he scope of implementation of this recommendation is being considered through electronic surveillance reform': AGD, *Submission 20*, 24.

860 The Intelligence Services Legislation Amendment Bill 2023 was introduced on 22 June 2023 and lapsed at dissolution of the 47th Parliament on 28 March 2025. A similar Bill, the Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2020, was introduced on 9 December 2020 and lapsed at dissolution of the 46th Parliament on 11 April 2022.

861 *ACIC Review* Recommendation 15. The government has accepted that recommendation, noting the need to 'align the ACIC's oversight arrangements with those of other agencies in the National Intelligence Community': AGD, *Government Response – Independent Review of the Australian Criminal Intelligence Commission and Associated Commonwealth Law Enforcement Arrangements* (November 2024) 3.

16.12 As this report was being finalised the Strengthening Oversight of the National Intelligence Community Bill 2025 (SONIC Bill) was introduced to parliament. This Bill substantially replicates the provisions of the former ISLAB Bill in relation to the division of responsibility for oversight of SLAID Act warrants between IGIS and Ombudsman.

16.13 Some submissions to this review supported the approach suggested by the 2019 Comprehensive Review.[862] Others suggested that IGIS should review all *SLAID Act* warrants.[863] AGD said that the current division of responsibilities for *SLAID Act* powers was 'broadly effective' and noted the ISLAB Bill 2023, which was at that time before the Parliament.[864]

16.14 The reviews mentioned above have generally considered oversight as a relatively small part of a much broader review focused on the role, powers and functions of law enforcement and intelligence agencies. The role, powers and functions of oversight bodies, including division of responsibilities, is a complex question and one that has implications well beyond *SLAID Act* warrants. A holistic look at the oversight system merits a review of its own.

16.15 For the purposes of this review, it has been assumed that there will be some kind of division of responsibility for *SLAID Act* warrants between IGIS and the Ombudsman. This is the current situation and would also be the result if the SONIC Bill is enacted. The remainder of this chapter focuses on relatively minor changes that should be made to enhance oversight of *SLAID Act* warrants regardless of the division of responsibilities.

Information sharing

16.16 Whatever division of responsibility is ultimately adopted, it is likely that there will be some form of overlap in the remit of the 2 oversight agencies. As the Ombudsman observed, 'overlap is preferable to jurisdictional gaps' and these overlaps should be managed by 'high levels of cooperation and information sharing.'[865]

16.17 Examples of overlapping jurisdiction and areas where a high level of cooperation and information sharing are important for *SLAID Act* warrants include the following:

- Currently, IGIS has oversight of the use of one type of AFP warrant and one type of ACIC warrant. The remainder of the powers and functions of those agencies, including other warrants used for the same operations, rests with Ombudsman:

862 For example, the Law Council indicated support for consolidating oversight of law enforcement related surveillance powers in the Ombudsman: Law Council, *Submission 23*, Recommendation 42; Brendan Walker-Munro, *Submission 3*, 14, Recommendation 12.

863 Philip Glover, *Submission 8*, 8. Dr Walker-Munro suggested that 'the Ombudsman have the mandate to conduct inspections in respect of the legal compliance for all *SLAID Act* warrants, whilst the IGIS inspect propriety': Brendan Walker-Munro, *Submission 3*, 15.

864 AGD, *Submission 20*, 23.

865 Ombudsman, *Submission 11*, 3.

- It is not possible for either oversight body to fully understand particular operations without being aware of issues that may have arisen with one part of the operation.
- It is difficult for the Ombudsman to exercise broader oversight of AFP or ACIC without knowing of systemic issues that may have arisen with NAWs.
- AFP and ACIC share information and can cooperate on operations where *SLAID Act* warrants may be used.

▲ If responsibility for the whole of ACIC moves to IGIS, as proposed by the ISLAB Bill and SONIC Bill, then IGIS and the Ombudsman will each have responsibility for the use of the same power (ATWs, and if Recommendation 1 is not accepted also DDWs) in different agencies:

- Sharing information about oversight of the same power as used by different agencies promotes consistency and efficiency in oversight.

16.18 I agree with the Ombudsman that 'as a general principle, it is highly desirable that oversight bodies that share jurisdictions have strong information sharing powers so that they are able to share information about potential systemic issues in relation to the use of covert and intrusive powers without this being inhibited by an inability to share agency-specific information.'[866]

16.19 Presently, there are some information sharing provisions that enable protected information to be communicated between Ombudsman officials and IGIS officials for the purpose of fulfilling their respective statutory functions.[867] IGIS said that these provisions 'appear sufficient whilst noting that there has been no need to make use of them to date in respect of [NAWs].'[868]

16.20 The Ombudsman noted that IGIS had advised that if responsibility for ACIC is transferred to IGIS then, after an 18-month transition period has passed, IGIS will not be permitted to share information with the Ombudsman.[869] This is clearly problematic if it presents a barrier to IGIS and the Ombudsman sharing information about how the same kinds of warrants are being utilised in different agencies. Further, sharing knowledge and advice about engineering questions that are relevant to the execution of powers that rely on technology will also enhance oversight and avoid duplication of effort in what is already a difficult area to build knowledge in.

866 Ombudsman, *Submission 11*, 5.

867 *SD Act* s 45(6A) (allowing Ombudsman official to communicate protected information to an IGIS official); *IGIS Act* s 32AC (allowing IGIS to share information with 'integrity bodies' defined to include the Ombudsman).

868 IGIS, *Submission 9*, 5 [14].

869 The Ombudsman's comments were in the context of the ISLAB Bill: Ombudsman, *Submission 11*, 5; the implications of the restrictive approach to information sharing under the ISLAB Bill were also canvassed before the PJCIS: IGIS, Submission No 7 to PJCIS, Parliament of Australia, *Review of the Intelligence Services Legislation Amendment Bill 2023* (4 September 2023) 13 [61]. There are similar transitional provisions about information sharing in the Strengthening Oversight of the National Intelligence Community Bill 2025.

16.21 With the introduction of PIMs and a technical advisors (see Chapters 8 and 9), it will also be necessary to ensure that IGIS and the Ombudsman (and their staff) are able to share information with those bodies in order to enhance the ability of all to perform their respective functions. IGIS did not foresee any difficulty in sharing information with the PIMs, subject to appropriate legislative and administrative mechanisms being put in place.[870] Similar legislative and administrative mechanisms would be needed for the Ombudsman and the technical advisors.

Recommendation 21: Oversight arrangements should be modified to reflect the following:

(a) There should be no statutory barriers to IGIS, the Ombudsman, PIMs and the technical advisors sharing information.

...

16.22 Information sharing between officials in the course of their duties should continue to be subject to normal Commonwealth security policies and secrecy offences.[871]

16.23 Before any future change to the division of oversight responsibilities is introduced, there should be careful consultation with oversight agencies (and in future PIMs and the technical advisory panel) to ensure that information sharing provisions are fit for purpose.

Access to technical advice

16.24 Increasing technological complexity 'will make it progressively more difficult for oversight bodies to understand the nature and operation of agencies' capabilities.'[872] In that context, if an oversight body is completely reliant on an agency it is overseeing for technical support, there is at the very least a risk to the perceived independence of oversight. In Chapter 9, I have explained my support for introducing independent technical advisors that have the capacity to provide independent advice to PIMs and issuing authorities on technology underpinning *SLAID Act* powers.

870 IGIS and INSLM, *Agreed Record of Meeting* (28 February 2025) 2

871 Department of Home Affairs, *Protective Security Policy Framework: Release 2024* (Policy, 18 December 2024); *Criminal Code* Part 5.6.

872 Department of the Prime Minister and Cabinet (Cth), *2024 Independent Intelligence Review* (Report, 2024), 116 [18.41] and 117, Recommendation 67.

16.25 Calls for access to independent technical advice for oversight bodies been made in the past.[873] As discussed in Chapter 9 the TAP in the United Kingdom performs such a role for both inspectors and issuing authorities, and its work is regarded as highly valuable by both. The Ombudsman supports having access to a technical advisory panel, as does IGIS.[874]

16.26 As a matter of efficiency, the same panel of experts that assists issuing authorities and PIMs should also provide advice to oversight and review agencies. Occasionally, the Monitor's reviews require understanding of technical issues and it would be beneficial if the Monitor could also access the technical advisory panel for advice.[875]

Recommendation 21: Oversight arrangements should be modified to reflect the following:

...

(b) Oversight bodies and the INSLM should have access to the proposed technical advisors.

...

16.27 There may also be opportunity for the same panel to be utilised in other statutory schemes that require similar advice.[876] The Australian Law Reform Commission should also be consulted about whether it may occasionally need to seek advice on specific reviews.

Removing unnecessary prescription

16.28 In relation to DDWs and ATWs, the Ombudsman is *required* to 'inspect the records' of AFP or ACIC to 'determine the extent of compliance' with the legislation by the agency or officers of the agency.[877] This contrasts with the more flexible jurisdiction of IGIS to look at matters of legality and propriety and to determine their own inspection schedule.

16.29 The Ombudsman would prefer that their inspection jurisdiction be less prescriptive and that it be modelled on the scope of 'matters of administration' that the Ombudsman can review and the issues they can report on under s 15 of the

873 *2024 Independent Intelligence Review* 117; see also *2019 Comprehensive Review,* vol 2, 281, Recommendation 173.

874 Ombudsman and INSLM, *Agreed Record of Meeting* (11 February 2025); IGIS and INSLM, *Agreed Record of Meeting* (28 February 2025). See also IGIS, *Annual Report 2023–24* (Report, 23 September 2024) 32.

875 The 2020 *TOLA Act* review required technical assistance: James Renwick, former Independent National Security Legislation Monitor, *Trust but Verify: A Report Concerning the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 and Related Matters* (Report, June 2020) 98 [5.2]. If referred, the AI review recommended by the 2024 review may similarly require advice: *2024 Independent Intelligence Review* 83, Recommendation 38.

876 See, for example, *Telecommunications Act 1997* (Cth) pt 15 (industry assistance).

877 *Crimes Act* s 3ZZVR (ATWs); *SD Act* s 55(1) (DDWs).

Ombudsman Act.[878] The Ombudsman said that such an approach would allow 'broader and more effective oversight than the current framework, which may be limited to reporting on agencies compliance with the Act(s).'[879] The Ombudsman 'sees significant value in this approach and opportunities for improvements in administrative practice in agencies as a result.'[880]

16.30 If such an approach were to be adopted, the range of matters that the Ombudsman could consider in inspections for *SLAID Act* warrants would be expanded and would include matters such as whether an action was contrary to law as well as whether it was unreasonable, unjust, oppressive or improperly discriminatory or otherwise wrong in all the circumstances.[881] This would be similar to the IGIS jurisdiction of 'legality and propriety.'

16.31 Part of the proposed change would be removing the mandatory inspection schedule and instead relying on the Ombudsman to determine their inspection regime, as IGIS does. Ombudsman noted that such an approach would 'allow more flexible and efficient allocation of limited inspection resources.'[882]

16.32 Both the Internet Association of Australia and the Law Council of Australia recommended that the Ombudsman be given broader inspection functions to evaluate the propriety of AFP and ACIC's *SLAID Act* powers.[883] The Law Council of Australia added that this should include an ability to undertake thematic reviews oversighting operations that used multiple warrant types. The proposed changes would allow this.

16.33 Neither AFP nor ACIC raised any concerns with the Ombudsman having a broader mandate to assess the 'propriety' of activities connected to *SLAID Act* powers, which was one of the specific questions in the issues paper for this review.[884] Both agencies noted that they work productively and cooperatively with oversight bodies.[885]

16.34 In addition to the current mandatory but limited inspections, the Ombudsman has power to undertake 'investigations'.[886] Own-motion investigations are generally major and resource-intensive reviews into areas where a problem is already suspected, often as a result of inspections or complaints.[887] There is a detailed set

878 Although 'matters of administration' are not defined in the *Ombudsman Act*, the Ombudsman indicated that 'it is well understood in the context of 47 years of the Commonwealth Ombudsman exercising its functions': Ombudsman, *Submission 11*, 4.
879 Ombudsman, *Submission 11*, 4.
880 Ombudsman and INSLM, *Agreed Record of Meeting* (11 February 2025) 2.
881 Ombudsman, *Submission 11*, 4; *Ombudsman Act* s 15.
882 Ombudsman and INSLM, *Agreed Record of Meeting* (11 February 2025) 2.
883 IAA, *Submission 16*, 5; Law Council, *Submission 23*, 65.
884 *Issues paper*, 54
885 ACIC, *Submission 17*, 10; AFP, *Submission 18*, 11.
886 *Ombudsman Act* s 5, 8.
887 See for example, ACT Ombudsman and Commonwealth Ombudsman, *Use of Force by ACT Police: More to Do to Lessen Harm* (Report, June 2025); Ombudsman, *Investigation into Compliance with the Public Interest Disclosure Act 2013* (Report, October 2022).

of requirements and extensive powers for 'investigations' in the *Ombudsman Act*.[888] IGIS has similar requirements and powers in relation to 'inquiries.'[889] As with the Ombudsman, IGIS inquiry powers are in addition to inspection functions.

16.35 In response to the proposal that the Ombudsman have a broader mandate for *SLAID Act* inspections, AGD highlighted that the Ombudsman could utilise their 'investigation' power to look at a broader range of issues.[890] This is true, but it is impractical as a replacement for a broader inspection mandate. The Ombudsman's resources are limited. Initiating an 'investigation' is, quite rightly, usually reserved for major issues and is not a substitute for routine inspections of covert powers. The department acknowledged that 'there may be opportunities to more closely align the Ombudsman's inspection and investigation functions, which the department will consider as part of the electronic surveillance reform.'[891]

16.36 It was also suggested that the agencies that the Ombudsman oversees are also subject to additional accountability through judicial and public scrutiny, differentiating them from those IGIS oversees.[892] For the reasons already discussed in this report, that is not so for covert powers, including *SLAID Act* powers, that are rarely going to result in evidence that can be challenged in court and where strict secrecy provision prevent public disclosure of any details their use.

16.37 The Ombudsman's remit under the *SD Act* is overly prescriptive and should be amended to give greater flexibility to determine how oversight resources are allocated. This could be achieved by removing the prescriptive requirements in the *Crimes Act* and *SD Act* and instead providing the Ombudsman with a mandate to conduct inspections to look at issues akin to those that the Ombudsman can examine in investigations.

888 *Ombudsman Act* s 8, 9, 12, 14, 14A, 15.
889 *IGIS Act* div 3.
890 AGD, *Submission 20*, 24.
891 AGD, *Submission 20*, 24.
892 AGD, *Submission 20*, 24.

16.38 This change is not dependent on the whether changes proposed by the SONIC Bill are made. Also, it is not dependent on any changes made as a result of the eventual findings of the electronic surveillance review, although it would be consistent with the findings of this report to make similar changes for inspection of electronic surveillance powers.

> **Recommendation 21: Oversight arrangements should be modified to reflect the following:**
>
> **...**
>
> **(c) Existing prescriptive requirements for Ombudsman inspections should be repealed and replaced by the ability to conduct inspections to examine matters akin to those that the Ombudsman can currently consider in 'investigations'.**
>
> **...**

16.39 This approach is consistent with the 2019 Comprehensive Review finding on oversight of electronic surveillance. The report recommended that legislation should allow oversight bodies to exercise discretion in managing their oversight functions and responsibilities and should avoid being 'overly prescriptive.'[893]

Record-keeping requirements

16.40 The *SD Act* and the *Crimes Act* require that AFP and ACIC keep certain records.[894] Amongst other things, these records facilitate oversight by ensuring there is an appropriate 'paper trail' setting out reasoning for key decisions. For example, AFP and ACIC must keep a record of any external communication of information collected by access to data held in a computer. This would include access obtained under a NAW or DDW.[895] These types of records are relevant to assessing compliance with the limits on information sharing in the legislation as well as in government policy (see the discussion in Chapter 17 about the sharing of death penalty and risk of torture information). Where oversight bodies have jurisdiction over the recipient of information (or can cooperate with a body that has jurisdiction), it would theoretically also allow inspections to assess whether any caveats or limits on the disclosed information were complied with. Similarly, records pertaining to when and how information was destroyed are essential to independent checking that destruction requirements have been adhered to.

893 *2019 Comprehensive Review*, vol 2 [31.22], [31.23]; vol 3, Recommendation 171.d.
894 *SD Act* ss 51-53; *Crimes Act* ss 3ZZVN, 3ZZVP.
895 *SD Act* s 52(1)(f)(ii). There is no equivalent provision in the *Crimes Act* for ATWs.

16.41 There are some inconsistencies with current specific statutory record-keeping requirements as they apply to the *SLAID Act* warrants. These are set out in Table 7.

Table 7 – Inconsistent record-keeping requirements across the SLAID Act powers

Record-keeping requirement	DDW	ATW	NAW
Assistance orders made[896]	✗	✓	✗
Each use and communication of information obtained under warrant by AFP or ACIC [897]	✓	✗	✓
Use and communication of information by other agencies	✗	✗	✗
Information obtained under warrant given as evidence in relevant proceedings [898]	✓	✗	✓
Destruction of information obtained under warrant [899]	✓	✗	✓

16.42 These inconsistencies may have arisen because the provisions for DDW and NAW warrants largely adopted the existing provisions in the *SD Act* for surveillance device warrants, and ATWs largely adopted those for search warrants in the *Crimes Act*. Thus, the provisions about record keeping seem to primarily derive from existing requirements for other warrants rather than specific consideration of the risks and needs of the *SLAID Act* powers.

16.43 The Australian Human Rights Commission, Dr Philip Glover and the Internet Association of Australia recommended that these inconsistencies be addressed.[900] The Law Council maintained its concerns about the need for strengthened requirements to keep records of assistance orders made to increase accountability for use of intrusive covert powers.[901] The Internet Association of Australia also raised concerns about the adequacy of existing requirements – for example, potential

896 *Crimes Act* s 3ZZVN(g) (ATWs).

897 *SD Act* s 52(1)(e)–(f). The requirements do not apply to secondary disclosures – for example, by an intelligence agency that AFP or ACIC give information to (DDWs): *SD Act* s 52(1)(e)–(f) (NAWs).

898 *SD Act* s 52(1)(g) (DDWs); although evidence cannot be obtained under an ATW, any incidental information obtained can be admitted in a non-criminal proceeding: *Crimes Act* s 3ZZVH(3)(k) (ATWs); *SD Act* s 52(g) (NAWs).

899 *SD Act* s 52(j) (DDWs and NAWs).

900 AHRC, *Submission 21*, 14, Recommendation 10; Philip Glover, *Submission 8*, 8; IAA, *Submission 16*, 5.

901 See also Law Council, Submission No 21 to PJCIS, Parliament of Australia, *Review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (9 March 2021) 113 Recommendations 35, 70; Law Council, *Submission 23*, Recommendation 52.

impacts on oversight because of agencies not being required to retain records about the destruction of information obtained under an ATW.[902]

16.44 More generally, the Law Council of Australia underlined the importance of ensuring 'consistent record-keeping requirements, to ensure that there is an audit trail of key decisions and activities' and 'making and keeping records of the reasoning underlying key decisions [where] … there is a choice between different surveillance powers.'[903]

> Without proper records it is not possible for an oversight agency to be satisfied that AFP or ACIC has in fact complied with its legal obligations and has acted with propriety.

16.45 The Ombudsman has raised specific concerns about record keeping relating to the exercise of *SLAID Act* powers.[904] I note that in other contexts the Ombudsman and IGIS have not infrequently criticised agencies for inadequate record keeping.[905] As a practical matter, it is already open to oversight agencies to provide non-binding guidance to AFP and ACIC on what sorts of records they expect to be made and retained.

16.46 Statutory record keeping requirements are inflexible and, as noted above, can be inconsistent. Administrative guidance given by oversight agencies is non-binding and may not be seen as sufficient. A system that allows binding administrative guidance to be given on what sorts of records are expected to be created and maintained by agencies allows more flexibility and detail than a legislative scheme can provide. To maximise transparency, guidance on what records are to be made and retained should be made public, except in so far as doing so would disclose operationally sensitive information. This approach will avoid overly prescriptive record-keeping requirements in legislation and, to that extent, is consistent with the approach recommended by the 2019 Comprehensive Review.[906] Clearly, there is a need for consultation with IGIS and the Ombudsman on what record-keeping requirements should be, as is consultation with agencies about what requirements are practical and how they can be implemented including through integration with electronic document management systems.

902 IAA, *Submission 16*, 5.

903 Law Council, *Submission 23*, 66 [251].

904 For example, the Ombudsman made findings about AFP's failure to keep a copy of each application for an ATW and potential sensitive material within the application: Ombudsman, *Report to the Attorney-General on Agencies' Compliance with the Crimes Act*: *2022–23 Controlled Operations Delayed Notification Search Warrants Account Takeover Warrant* (Report, November 2023), 23.

905 See, for example, concerns about unexecuted warrants and the need for agencies to better record decisions to retain or revoke them: Ombudsman, *Surveillance Device Powers: Are Agencies Complying?* (Report, September 2024) 16. In relation to IGIS, see comments on the need for improved record keeping by intelligence agencies (not including AFP and ACIC): IGIS, *Annual Report 2023–24* (Report, 23 September 2024) 80, 83, 86, 96–7, 102, 107, 111.

906 2019 Comprehensive Review, vol 3, 271, Recommendation 171; AGD, *Submission 20*, 28.

16.47 As noted in Chapter 12, there are different mechanisms for giving binding administrative guidance, including through the UK system of codes of practice and guidelines issued by a Minister.[907]

> **Recommendation 21: Oversight arrangements should be modified to reflect the following:**
>
> **...**
>
> **(d) Prescriptive statutory *record-keeping* and notification requirements should be replaced by a scheme that allows for binding administrative guidance to be given and updated as required.**
>
> **...**

16.48 Noting that the record-keeping requirements for *SLAID Act* warrants are modelled on those for electronic surveillance and computer access under a search warrants, it may be most efficient if this change was implemented as part of the electronic surveillance review.

16.49 In the interim, AFP and ACIC should continue to follow any guidance from IGIS and the Ombudsman on record keeping, including for *SLAID Act* warrants.

Notification requirements

16.50 In addition to keeping records and annual reporting, AFP and ACIC are required to notify IGIS or the Ombudsman of certain actions. There are some inconsistencies in these requirements, as outlined in Table 8.

16.51 Some of the variations in notification requirements for *SLAID Act* powers are consistent with 'the different purposes and effects of the powers.'[908] For example, as noted by AGD, for DDWs material damage must be reported, but this is not the case for NAWs and ATWs, because causing material loss or damage is not authorised under NAWs or ATWs.[909]

907 Given their responsibility for integrity, any ministerial guidelines relating to effective oversight by relevant oversight agencies should be made by the Attorney-General. As a minimum, AFP and ACIC, as well as IGIS and the Ombudsman, should be consulted before any binding guidance is finalised or amended.

908 AGD, *Submission 20*, 27.

909 AGD, *Submission 20*, 27.

Table 8 – Inconsistent notification requirements across SLAID Act warrants

Requirement to notify the Commonwealth Ombudsman or IGIS	DDW	ATW	NAW
Of warrant within 7 days of warrant being issued[910]	✓	✗	✓
If warrant is extended, varied or revoked[911]	✗	✗	✓
Of concealment of activities done under warrant[912]	✗	✗	✓
Within 7 days if activity authorised by warrant has caused material loss or damage[913]	✓	N/A	✓

16.52 The Australian Human Rights Commission, Dr Glover, the Internet Association of Australia and the Law Council of Australia said that inconsistencies in notification requirements should be addressed.[914] The Law Council of Australia reiterated earlier concerns that they had raised about the absence of notification requirements for post-warrant concealment activities under DDWs, pointing out that notification is critical to providing relevant oversight agencies notice of high risk operations.[915]

16.53 IGIS found that in a small number of cases AFP and ACIC did not meet the required notification timeframe for reporting the extension of a NAW.[916] IGIS also raised concerns about the difference in the level of detail provided by agencies when notifying that a NAW is issued, extended, varied or revoked or that a concealment activity is undertaken.[917] Further, IGIS said that the absence of an express requirement to provide copies of the affidavit underpinning NAW applications has meant that they have had to be requested, resulting in less timely oversight.

910 *SD Act* s 49C(1), s 27KM(3).
911 *SD Act* ss 26KQ(7), 27KR(6)–(7).
912 *SD Act* ss 49D, 27KP(8)(c), 27KP(k)–(l).
913 *SD Act* ss 27KP(6)(b), (9)(b), 49(2D)(d)(viii), 49(2E)(x); *Crimes Act* ss 3ZZUR(5)(b), (7)(b), 3ZZVN(g).
914 AHRC, *Submission 21,* 14; Dr Glover, *Submission 8*, 8; IAA, *Submission 16*, 5; Law Council, *Submission 23*, [252]–[253] and Recommendation 44.
915 Law Council, *Submission 23*, 67.
916 IGIS, *Annual Report 2023–24* (Report, 2024) 113.
917 IGIS, *Submission 9*, 5.

In practice, agencies have provided copies of affidavits wherever requested.[918] The Ombudsman did not consider further notification requirements were required, as its powers to inspect and obtain relevant information were 'sufficient to identify and report on issues.'[919]

16.54 The 2019 Comprehensive Review found, '[n]otification requirements do not need to be prescribed in legislation, to allow oversight bodies flexibility to prioritise the powers that pose the greatest risk.'[920] In a similar vein, the Law Council of Australia noted that 'rigid and extensive statutory notification obligations can impose a significant burden on investigative agencies … and on the relevant oversight bodies.'[921]

16.55 As with record-keeping requirements, there is scope for guidance to be given to AFP and ACIC on when oversight bodies are to be notified of specific occurrences and how much detail they require. These requirements may change over time. For example, a new power, the use of a new capability or identification of an area where previous noncompliance has been a concern may require prompt notification and considerable detail, whereas the use of established powers and technologies by an agency with a strong history of compliance may not need specific notification or may only require notification on agreed schedule.

16.56 I recommend that the same approach proposed above in relation to record keeping also be adopted for notification requirements. That is, detailed statutory requirements should be replaced by a statutory scheme that allows for binding administrative guidance to be issued and updated whenever required. Given that notification to oversight agencies is very specific to those agencies, as opposed to record keeping, which also serves other purposes, consideration could be given to whether IGIS and the Ombudsman, rather than a Minister, should issue guidance on notification. This is not an option that was raised with IGIS or the Ombudsman in this review, and further consultation should be undertaken if it is to be IGIS or the Ombudsman that gives notification rather than a Minister after consulting those agencies.

Recommendation 21: Oversight arrangements should be modified to reflect the following:

…

(d) Prescriptive statutory record-keeping *and notification* requirements should be replaced by a scheme that allows for binding administrative guidance to be given and updated as required.

…

[918] IGIS and INSLM, *Agreed Record of Meeting* (28 February 2025) 4.
[919] Ombudsman, *Submission 11*, 6.
[920] *2019 Comprehensive Review*, vol 3, 270.
[921] Law Council, *Submission 23*, 67.

16.57 In the interim, AFP and ACIC should continue to follow any guidance from IGIS and the Ombudsman on notification, including what material should be included with notices for *SLAID Act* warrants.

Public reporting of oversight findings

16.58 The way that IGIS and the Ombudsman report on findings of their *SLAID Act* inspections differs. If IGIS prepares an inspection report on NAWs, it can only be provided to the Minister responsible for the agency or the head of the agency.[922] The IGIS annual report must include 'comments' on any inspections conducted in the relevant year.[923] In contrast, the reports of each Ombudsman inspection of DDWs and ATWs are provided to the relevant Minister, who must table them in Parliament.[924] If responsibility for oversight of all of ACIC is transferred to IGIS there will be less public reporting, including about inspections of *SLAID Act* warrants under the current legislative scheme.

16.59 The 2019 Comprehensive Review said that copies of oversight body reports should be tabled in Parliament, subject to redactions to avoid prejudice to security, the defence of Australia, Australia's relations with other countries, law enforcement operations and the privacy of individuals or to avoid danger to a person's safety. It also said that, in general, oversight bodies should be able to publish their unclassified reports at any time.[925] Further, it said that oversight bodies should be able to brief parliamentary committees both when they consider it necessary and at the committee's request.[926] I support this approach.

922 *IGIS Act* s 25A.
923 *IGIS Act* s 35(2A).
924 *SD Act* s 61(1) and (2); *Crimes Act* s 3ZZVX. It is the Ombudsman's preference that reports to the Minister continue to be tabled in Parliament: Ombudsman and INSLM, *Agreed Record of Meeting* (11 February 2025), 2.
925 *2019 Comprehensive Review*, vol 2, 442 [31.53] and Recommendation 132.
926 *2019 Comprehensive Review*, vol 3, [40.132]–[40.133].

16.60 It follows that there should be more scope than there currently is for IGIS to publish unclassified findings from review of *SLAID Act* powers at any time. The secrecy provisions in the *IGIS Act* are subject to some uncertainty and it is not clear whether IGIS can publish unclassified versions of inspection or inquiry reports throughout the year.[927] This should be amended to allow IGIS greater latitude in public reporting.

Recommendation 21: Oversight arrangements should be modified to reflect the following:

...

(e) IGIS and the Ombudsman should be able to brief parliamentary committees and IGIS should be able to publish unclassified inspections reports and inquiries at any time.

...

16.61 There is currently provision for the Minister to redact certain information from IGIS annual reports.[928] There is an obligation on the Ombudsman to not include certain sensitive information in ATW inspection reports that are tabled in Parliament.[929] However, there is no corresponding obligation on the Ombudsman to not include sensitive information in relation to DDWs.[930] Although there is no suggestion that the Ombudsman would include this type of information, this discrepancy should be addressed. Also, there should be consistent obligations on the Ombudsman to not include sensitive information on both ATWs and DDWs in reports that are to be made public.

16.62 In practice, IGIS and the Ombudsman consult with agencies to seek advice on information that may cause harm if disclosed. They will seek to negotiate an agreed form of words to describe potentially sensitive material in public reports in a way that does not cause harm to operations (etc.).

927 *IGIS Act* s 34. I note that different Inspectors-General have taken different approaches to publishing unclassified reports.

928 *IGIS Act* s 35(5) allows deletion of information that the Attorney-General considers may prejudice security, defence, relations with other countries, law enforcement operations of the privacy of individuals.

929 *Crimes Act* s 3ZZVX requires that the report not include information which, if made public, could reasonably be expected to prejudice an investigation or prosecution or compromise operational activity or methodologies.

930 In accordance with s 61 of the *SD Act*, information in an inspection report relating to a 'computer access warrant' or a 'surveillance device warrant' (categories that do not include DDWs) can be removed, but only if the information is 'Part 5.3 information' or 'Part 9.10 information.' Broadly, these refer to certain post-sentence orders to do with terrorism (pt 5.3 of the *Criminal Code*) or community safety orders (pt 9.10 of the *Criminal Code*).

Recommendation on oversight

Recommendation 21: Oversight arrangements should be modified to reflect the following:

(a) There should be no statutory barrier to IGIS, the Ombudsman, PIMs and the technical advisors sharing relevant information.

(b) Oversight bodies and the INSLM should have access to the proposed technical advisors.

(c) Existing prescriptive requirements for Ombudsman inspections should be repealed and replaced by the ability to conduct inspections to examine matters akin to those that the Ombudsman can currently consider in 'investigations'.

(d) Prescriptive statutory record keeping and notification requirements should be replaced by a scheme that allows for binding administrative guidance to be given and updated as required.

(e) IGIS and the Ombudsman should be able to brief parliamentary committees and IGIS should be able to publish unclassified inspections reports and inquiries at any time.

(f) There should be consistent obligations on the Ombudsman to not include sensitive DDW or ATW information in public reports.

Part 7. SLAID Act powers and Australia's international obligations

Reviews by the Monitor must have regard to Australia's obligations under international agreements.[931] Particularly relevant to this review are human rights obligations under the *ICCPR*; obligations and norms around not interfering with the territory or sovereignty of other States; and specific agreements relating to cybercrime. This Part briefly summarises key obligations and concludes that:

- there are several measures already recommended elsewhere in this report that, if implemented, will improve compliance with human rights obligations, including rights concerning privacy, fair hearing and an effective remedy
- the current position of requiring consent from the relevant country for warrants to be granted when it is *known* that the data to be disrupted or obtained is in that country should be retained. Consideration should be given to extending this requirement to the takeover of accounts, at least for accounts belonging to people *known* to be outside Australia where the service the account allows access to is also known to be hosted outside Australia
- international legal norms about extraterritorial operation of warrants in relation to cybercrime are evolving and it may be necessary to revisit issues associated with extraterritoriality
- there should be administrative arrangements in place to ensure that AFP and ACIC consult with the Department of Foreign Affairs and Trade in relation to foreign relations risks in appropriate cases.

931 *INSLM Act* s 8.

Chapter 17: International human rights obligations

17.1 Intelligence gathering, account takeover and disruption of crimes all have the potential to enhance some human rights and infringe others.

17.2 Infringement of rights, including the right to privacy, needs to be proportionate. Many of the key recommendations already made in this report are directly relevant to the question of whether rights-infringing activity is proportionate. This chapter looks at key rights that may be infringed by *SLAID Act* powers and how the recommendations in this report can assist in ensuring compliance with Australia's international human rights obligations.

Use of SLAID Act powers can protect rights

17.3 Combating serious crime, including through the appropriate use of *SLAID Act* powers, may promote multiple rights, including the rights to life and security of the person and the rights of the child.[932]

17.4 The right to life imposes an obligation on the State to protect people from not only direct threats to life but also 'reasonably foreseeable' threats to life, including terrorism and organised crime.[933] This requires Australia to enact a protective legal framework and take positive measures to address general conditions in society that give rise to reasonably foreseeable risks to the right to life, such as reducing the 'proliferation of potentially lethal weapons to unauthorized individuals.' There is an obligation to investigate and prosecute perpetrators of alleged violations of the right to life, even where the threat to life did not materialise.[934]

17.5 The right to security of the person is broader than the right to life, requiring the State to take steps to protect people against interference with personal integrity by others. This includes protecting people who are subject to death threats, assassination attempts, harassment and intimidation.[935]

932 *ICCPR* art 6(1) and 9(1); *Convention on the Rights of the Child*, opened for signature 20 November 1989, 1577 UNTS 3 (entered into force 2 September 1990) arts 19, 34–6 (*Convention on the Rights of the Child)*; PJCHR, *Human Rights Scrutiny Report* (Report No 3 of 2021, 17 March 2021) (*PJCHR Report No 3 2021*) 67 [2.56].

933 *ICCPR* art 6(1). Human Rights Committee, *General Comment No 36 on Article 6: Right to Life*, 120th sess, UN Doc CCPR/C/GC/36 (14 July 2015, adopted 30 October 2018) [3], [18] (*UNHRC General Comment on Article 6*).

934 *UNHRC General Comment on Article 6* [21], [27].

935 Human Rights Committee, *General Comment No 35 on Article 9, Liberty and Security of Person*, 112th sess, UN Doc CCPR/C/GC/35 (25 October 2012, adopted 31 October 2014) [9].

17.6 Australia has an obligation to protect children from all forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or exploitation, including sexual exploitation and abuse. This includes a positive obligation to take preventative measures, including identification, reporting, referral and investigation, of instances of potential violation of the rights of the child.[936]

17.7 Measures to protect these human rights need to be implemented in a way that does not detract from other rights in an impermissible way.

Use of SLAID Act powers can infringe rights

17.8 The use of *SLAID Act* powers can infringe human rights – most obviously the right to privacy.[937] Other rights, including the right to a fair hearing and the right to an effective remedy, are also engaged by the use of *SLAID Act* powers.[938] The prohibition against torture and other cruel, inhuman or degrading treatment or punishment is also potentially engaged if information is shared with countries where this is a risk.[939] Apart from the prohibition against torture (etc.) which is an absolute right, other rights may be limited if the limitation is prescribed by law, seeks to pursue a legitimate objective, is likely to be effective to achieve that objective (rationally connected) and is proportionate.[940]

17.9 Protecting Australians from cyber-enabled serious and organised crime is a legitimate objective.[941] As I have explained in Chapter 2, *SLAID Act* powers can be effective in supporting that objective. The key question is whether *SLAID Act* powers are a *proportionate* way of achieving this goal. Assessing this requires considering relevant rights individually and looking at the *SLAID Act* scheme holistically.

> Protecting Australians from cyber-enabled serious and organised crime is a legitimate purpose, and the *SLAID Act* powers are likely to be effective in achieving that objective. The key question is whether *SLAID Act* powers are *proportionate*.

Right to privacy

17.10 Article 17(1) of the *ICCPR* provides for every person to be protected against arbitrary or unlawful interference with their privacy, family, home or correspondence. The

936 *Convention on the Rights of the Child* arts 19, 34–36.
937 *ICCPR* art 17(1).
938 *ICCPR* arts 2(3), 14.
939 *ICCPR* art 7; *Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment*, opened for signature 10 December 1984, 1465 UNTS 85 (entered into force 26 June 1987), art 3(1).
940 PJCHR, Parliament of Australia, *Guide to Human Rights* (Guide, June 2015), 7 [1.15]. AHRC, *Submission 21*.
941 AGD, *Submission 20*, 28–9; AHRC, *Submission 21*, 14 [48].

United Nations Human Rights Committee has explained that the expression 'arbitrary interference' means that any limitation must be authorised by law and 'in accordance with the provisions, aims and objectives of the [ICCPR] and should be, in any event, reasonable in the particular circumstances.'[942] In the context of the *European Convention on Human Rights*, which has a similar provision, it has been said that, for covert surveillance, a test of 'strict necessity' is to be applied in light of an elevated risk to interfere with privacy:

> given the particular character of the interference in question and the potential of cutting-edge surveillance technologies to invade citizens' privacy, the Court considers that the requirement 'necessary in a democratic society' must be interpreted in this context as requiring 'strict necessity'.[943]

17.11 The Australian Human Rights Commission, and civil society groups, argued that several aspects of the *SLAID Act* regime risked disproportionate interference with the right to privacy – for example:

- whether the use of the powers is restricted to sufficiently serious crimes[944]
- impacts on persons not subject to investigation[945]
- the independence and expertise of the person issuing the warrants, including whether warrants are issued by a judge and whether they have the benefit of a PIM or similar contradictor and access to independent technical advice[946]
- whether the criteria to be applied in issuing warrants and authorisations provides for appropriate safeguards in regards to privacy rights[947]
- whether there are enough safeguards applying to the life cycle of data.[948]

17.12 These factors are all relevant to the proportionality of *SLAID Act* powers in the sense of the right to privacy. They are also relevant to the general proportionality of *SLAID Act* powers and the protection of individual rights in the sense of s 6(1)(b) of the *INSLM Act*. As such, each of these points has already been considered in this report and relevant recommendations have already been made. This includes:

942 Human Rights Committee, *CCPR General Comment No 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 32nd sess, UN Doc HRI/GEN/1/rev.6 (8 April 1988) [4].

943 *Szabó and Vissy v Hungary*, European Court of Human Rights, App no 37138/14 (2016) 38–9 [73].

944 See, for example, QCCL, *Submission 6*, 2; AJF, *Submission 7*, 2–3 [2.4], [2.9]; AHRC, *Submission 21*, 5 [14]; Law Council, *Submission 23*, 16 [34]; HRLC, *Submission 5*, 6; Digital Rights Watch, *Submission 22*, 5.

945 See, for example, HRLC, *Submission 5,* 9; AHRC, *Submission 21*, 6 [17].

946 See, for example, QCCL, *Submission 6*, 6; Joint Academic Submission, *Submission 15*, 8; AHRC, *Submission* 21, 8 [26]; Law Council, *Submission 23*, 16 [34].

947 See, for example, Civil Liberties Australia, *Submission 4*, 1; AHRC, *Submission 21*, 9 [30]; Law Council, *Submission 23*, 49–50 [179]–[184].

948 See, for example, HRLC, *Submission 5*, 10; QCCL, *Submission 6*, 8; AJF, *Submission 7* 6; AIIA, *Submission 12*, 5; Joint Academic Submission, *Submission 15*, 8–9; AHRC, *Submission 21*, 12 [40]; Law Council, *Submission 23*, 51–2 [192]–[193], 56–7 [214]–[217].

- *SLAID Act* warrants being issued by retired judges, if that is not agreed then judges (Recommendation 6)
- strengthening the system for issuing warrants to include PIMs (Recommendation 7), an effective secretariat, access to a technical advisory panel, and a statutory duty of candour on warrant applicants (Recommendation 8)
- *SLAID Act* warrants being available only in relation to offences carrying a penalty of 5 or more years (Recommendation 9)
- ensuring that privacy, property rights and the need for safeguards for sensitive categories of data are considered in all warrant applications (Recommendation 12).

17.13 If these measures are adopted, it is not necessary to make additional recommendations to strengthen compliance with Australia's obligations under art 17(1).

Implementation of recommendations in this report relating to a new system for issuing warrants, improved issuing criteria and new protections for personal information will significantly improve compatibility with the right to privacy.

Right to a fair hearing

17.14 Article 14(1) of the *ICCPR* provides for everyone to be entitled to a 'fair and public hearing by a competent, independent and impartial tribunal established by law.' Article 14(3) of the *ICCPR* sets out certain minimum guarantees in relation to criminal process rights. There are 2 main issues for art 14 and *SLAID Act* warrants: the risk of 'disrupted' data being used in evidence; and the difficulty of challenging evidence because of provisions that allow information about the technology and methodologies used to execute warrants to be suppressed in a trial. A potential third issue is whether the current secrecy provisions prevent disclosure of potentially exculpatory material. This is most relevant to NAWs and Recommendation 14(e) specifically says that an amendment is needed to ensure exculpatory maternal can be disclosed.

17.15 The Law Council of Australia raised concerns about the risk that data modified by a DDW might be adduced as evidence. In particular, the Law Council was concerned that a defendant may have difficulty challenging the admissibility of evidence because it may not be 'technically possible to readily identify and quantify the impacts of a data disruption activity on the integrity, accuracy and reliability of evidence about the online activities of suspects and others.'[949] To address these concerns, the Law Council recommended amendments to the *SD Act* to provide that information obtained under a DDW cannot be admissible in criminal

949 Law Council, Submission No 21 to the PJCIS, Parliament of Australia, *Review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (9 March 2021) 97 [321].

proceedings against a person for the relevant offence specified in the DDW.[950]

17.16 Given that the primary purpose of DDWs is disruption, it is unlikely that information collected under those warrants will be used in evidence (see Chapter 2). This will be further reinforced by Recommendation 13 – that DDWs only be available as a 'last resort' when, for example, prosecution is not believed to be a viable option. Nevertheless, it is possible that while executing a DDW evidence might be obtained and, despite an earlier belief that a prosecution was not feasible, proceedings may be commenced. If this situation were to arise, a judge would have to grapple with the admissibility of the evidence, including the risk that data may have been modified. In such a situation the primary safeguard would be the existing rules of evidence, established expectations about the chain of evidence and the prosecutorial duty of disclosure. Although it may be difficult for a defendant to challenge evidence where technically complex means were used to gather it, this alone is not enough of a reason for a change to the rules of evidence or to introduce a requirement to automatically exclude evidence.

> The risk of modified data collected under a DDW being adduced in evidence in a way that is in breach of the right to a fair hearing can be managed with existing rules.

17.17 A potential situation where it may be effectively impossible for a defendant to challenge evidence is where orders are made to prevent disclosure of information that could reveal data disruption, computer access and account takeover technologies or methods. The *SLAID Act* provisions allow for these types of orders to be sought and made.[951] In making this type of order, the person presiding over the proceeding must take into account whether disclosure is necessary for the fair trial of the defendant.[952] It is probably both unnecessary and undesirable to have a separate specific power to make orders in relation to *SLAID Act* technologies and methods rather than rely on the general scheme of protecting sensitive information in the *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth).[953] Nevertheless, the power in the *SLAID Act* provisions is not inconsistent with the right to a fair trial because it is clear that the power is to be exercised subject to the requirement that the defendant receive a fair trial.

950 Law Council, *Submission 23*, 56, Recommendation 31.

951 *SD Act* ss 47A, 47B; *Crimes Act* s 3ZZVK.

952 *SD Act* ss 47A(3), 47B(3); *Crimes Act* s 3ZZVK(3).

953 The *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth) (*NSI Act*) protects 'national security' information in civil and criminal proceedings. The definition of 'national security' includes 'law enforcement interests,' which expressly includes 'protecting the technologies and methods used to collect, analyse, secure or otherwise deal with, criminal intelligence, foreign intelligence or security intelligence': *NSI Act* s 11. The *NSI Act* is out of scope for this review, but see Grant Donaldson, former Independent National Security Legislation Monitor, *Review into the Operation and Effectiveness of the National Security Information (Criminal and Civil Proceedings) Act 2004* (Report, 30 October 2023).

Right to an effective remedy

17.18 Article 2(3) of the *ICCPR* requires States to ensure access to an effective remedy for violations of human rights. There are several limitations on the ability to provide a right to an effective remedy in the context of actions taken under covert warrants.

17.19 Unlike search warrants, *SLAID Act* warrants are issued without notice to impacted individuals at any stage. The Joint Academic Submission noted:

> [This is] highly unusual in policing, where a person will generally become aware of a warrant upon its execution and, at that point, have an opportunity to raise concerns and questions regarding the warrant, to consider legal action seeking an injunction or other remedy, and to make any relevant assertions of privilege.[954]

Judicial review is unlikely

17.20 The Revised Explanatory Memorandum said the availability of judicial review of the issuing of a *SLAID Act* warrant is a mechanism for ensuring that an affected person has an avenue to challenge decisions made under the *SLAID Act*.[955] In practice this is unlikely to be an effective remedy because an affected person is unlikely to be aware of the use of these covert powers.

17.21 An opportunity to challenge actions relating to the execution of covert warrants may arise if information collected under those warrants is being adduced as evidence. However, this is also likely to be of limited practical application for *SLAID Act* warrants. Information collected under a NAW is generally not admissible in criminal proceedings, the primary purpose of a DDW is disruption rather than the collection of evidence, and the primary purpose of an ATW is to facilitate access so that evidence can be collected under other powers.

> Judicial review is unlikely to be a practical remedy for a covert warrant that the affected person is unaware of.

What is available in absence of a judicial remedy?

17.22 Oversight processes (Chapter 16) can lead to a 'remedy' in certain circumstances. If the IGIS or the Ombudsman found that a warrant had been sought on an improper basis (for example, there was a breach of the duty of candour) or that a warrant had been exercised in a way that exceeded its authority or improperly infringed rights, they may recommend remedial action which could potentially include

954 Joint Academic Submission, *Submission 15*, 6.
955 Revised Explanatory Memorandum, 19 [51].

compensation.[956] Both IGIS and the Ombudsman can initiate reviews of their own motion as well as in response to complaints. Clearly own-motion powers are particularly important in relation to the exercise of covert warrants.[957]

Review by oversight agencies can lead to remedial action, although there are significant limits.

17.23 There are some limitations to the extent to which these oversight mechanisms provide an effective remedy to a person whose rights have been affected by the execution of a *SLAID Act* warrant. As highlighted by the PJCHR, general administrative oversight mechanisms (which would include IGIS and the Ombudsman) that do not give the affected individual their rights do not meet the requirement under art 2(3).[958]

17.24 Remedial action recommended by an oversight body is not the same as an individual having a right to pursue a remedy, and recommendations by IGIS and Ombudsman are not enforceable.[959] There are also limitations on the material that oversight agencies can disclose directly to an affected person. This is likely to operate as a significant practical barrier and may prevent disclosure of a finding to the affected person.[960]

17.25 The Australian situation may be contrasted with the United Kingdom, where the Investigatory Powers Commissioner can require an intelligence or law enforcement agency to notify persons adversely affected by a serious 'relevant error' made by that agency in the exercise, or purported exercise, of its equipment interference powers.[961] The person can then bring an action in the Investigatory Powers Tribunal

956 The *IGIS Act* expressly allows the Inspector-General to recommend compensation for a person adversely impacted by a Commonwealth agency: *IGIS Act* s 22(2). The Ombudsman does not have a specific power but may recommend some action should be taken to 'rectify, mitigate or alter the effects of a decision' and has made such recommendations in the past in other contexts: *Ombudsman Act* s 15(2), Ombudsman and INSLM, *Agreed Record of Meeting* (11 February 2025).

957 *IGIS Act* s 8(3A); *Ombudsman Act* s 5(1).

958 *PJCHR Report No 3 2021*, 95–8 [2.93]-[2.96], [2.102].

959 *IGIS Act* s 22(2)(b); *Ombudsman Act* s 15(2).

960 This includes restrictions on the ability to disclose the existence of a warrant: *Crimes Act* ss 3ZZUK (definition of 'protected information'), 3ZZVH; *SD Act* ss 44(1)(b)(i), 44A(c), 45, 45B. There is an additional layer of complexity in the intersection between the Ombudsman's ability to prepare public-facing reports on matters it investigates (under s 15 of the *Ombudsman Act*) and the *SLAID Act* secrecy provisions. Similarly the *IGIS Act* secrecy provisions that allow disclosure to a complainant are only triggered by a complaint and are limited if disclosure may prejudice an investigation: *IGIS Act* s 23.

961 *Investigatory Powers Act 2016* (UK) s 231. Before deciding whether the inform a person, the Investigatory Powers Commissioner must consider certain matters, including the extent to which disclosing the error would be contrary to the public interest or prejudicial to the prevention or detection of serious crime: *Investigatory Powers Act 2016* (UK) s 231(4).

seeking a remedy.[962] As discussed in Chapter 16, the structure of oversight arrangements in the United Kingdom is quite different from that in Australia. The introduction of a similar body to the Investigatory Powers Tribunal would be a significant improvement to satisfying the right to an effective remedy. It would also be a major change to Australia's oversight arrangements and have implications well beyond the oversight of *SLAID Act* warrants and would require careful review and consultation, and is beyond the scope of this review.

17.26 As outlined above, concerns about the proportionality of infringements of the right to privacy may be addressed to some extent by the creation of a PIM (Recommendation 7) who can draw attention to potential violations of human rights and challenge them if they are not necessary or proportionate. PIMs can also raise any earlier findings by oversight bodies that may point to systemic issues or other reasons to not issue a warrant or to impose conditions. However, PIMs cannot (and should not) be regarded as acting for an individual who is the subject of a warrant. Also, it is not their role to provide a remedy to individuals.

17.27 For emergency authorisations, if Recommendation 17(b) is implemented, the issuing authority will be given discretion to order that improperly collected data be destroyed. While that may be seen as a 'remedy' of sorts, it is still an administrative remedy and not one the affected person can themselves seek – or probably even know about.

The rights that are likely to be adversely affected by *SLAID Act* powers will be better protected if the recommendations from this review are implemented, reducing the need for an effective remedy. The availability of oversight agencies to recommend remedial action may provide a 'remedy' of sorts in some situations, but it does not satisfy the right to an effective remedy. A model similar to the United Kingdom Investigatory Powers Tribunal could be considered in a future review.

Right to life and prohibition against torture

17.28 The risk of Australian authorities using *SLAID Act* warrant information in a way that may contribute to an infringement of the right to life (through the imposition of the death penalty) or the prohibition against torture (etc.) is most likely to arise from the primary or secondary disclosure of information to foreign countries, particularly those that have the death penalty or a poor human rights record.[963]

962 The Investigatory Powers Tribunal is a judicial body that considers complaints and proceedings relating to alleged unlawful action use of covert investigative techniques by public agencies (predominantly intelligence agencies): see *Regulation of Investigatory Powers Act 2000* (UK) s 65.

963 See *PJCHR Report No 3 2021*, 103–11; *Second Optional Protocol to the International Covenant on Civil and Political Rights, aiming at the abolition of the death penalty*, GA res 44/128, UN GAOR, UN Doc A/RES/44/128 (15 December 1989).

17.29 The Australian Human Rights Commission argued that legislation should expressly require that protected information must not be shared with a foreign country 'where there are substantial grounds for believing there to be a real risk that disclosure of information to a foreign country may expose a person to the death penalty or to torture or cruel, inhuman or degrading treatment or punishment.'[964]

17.30 AGD said there are several mechanisms with similar effect that already exist, including AFP and ACIC policies and guidelines that limit those agencies' cooperation with overseas law enforcement agencies in international crime prevention as it relates to both the death penalty and torture.[965] Publicly available AFP policies set out procedures when officers believe that cooperation could lead to an individual being 'detained, arrested, charged or prosecuted' for an offence carrying the death penalty or where an individual is at risk of torture (etc.).[966] ACIC 'must act in accordance with the ACIC Death Penalty and Foreign Disclosure Policy (which broadly aligns to AFP's National Guideline on international police-to-police assistance in potential death penalty situations).'[967]

17.31 The primary external mechanism for checking adherence to limits on sharing information in a way that could contribute to violation of these rights is the oversight of IGIS and the Ombudsman. Clearly this requires more than inspecting warrant applications and reports, but these types of inquiries are within the remit of IGIS and the Ombudsman for the agencies they oversee regardless of whether there is an express statutory rule or not.[968]

17.32 I have already recommended that the issuing criteria for *SLAID Act* warrants be amended to require the issuing authority to consider necessity and proportionality in all the circumstances, including the adequacy of agency policies such as those about the retention and sharing of special categories of information (Recommendation 12(e)). Clearly, where it appears relevant, this can include the adequacy of policies that are intended to safeguard against the sharing of information that could be used in a way contrary to Australia's position on the death penalty or contrary to the prohibition on torture (etc.). If this recommendation is implemented then both PIMs and issuing authorities will regularly be considering the adequacy of policies, along with any relevant oversight findings as part of the overall assessment of the necessity and proportionality of issuing a *SLAID Act* warrant. This is a meaningful additional safeguard, although I recognise that it does not go as far as the Australian Human Rights Commission would like.

964 AHRC, *Submission 21*, 15–16, Recommendation 12. This recommendation reiterated an earlier PJCHR recommendation to the same effect: see *PJCHR Report No 3 2021*, 111 [2.138].

965 AGD, *Submission 20*, 22, 29–30. This includes safeguards in the *Mutual Assistance in Criminal Matters Act 1987* (Cth) and s 59AA(1)(f) of the *ACC Act*.

966 AFP, *AFP National Guideline on International Police-to-police Assistance in Death Penalty Situations* (Guideline); and AFP, *AFP National Guidelines on Offshore Situations Involving Potential Torture or Cruel, Inhuman or Degrading Treatment or Punishment* (Guideline). See also AGD, *Submission 20*, 29.

967 AGD, *Submission 20*, 29–30 and email from ACIC to INSLM, 18 July 2025.

968 For IGIS both inspections and inquiries could address this topic: *IGIS Act* ss 8(3A), 9, 9A. See, for example, IGIS, *Annual Report 2022–23* (Report, 25 September 2023). For the Ombudsman amendments are required to broaden inspection powers (see Chapter 16) but existing investigation powers would apply: *Ombudsman Act 1976* (Cth) s 5(1).

Under the proposed new system, issuing authorities and PIMs should be regularly considering the adequacy of policies that are intended to safeguard against the sharing of information that could be used in a way that is contrary to Australia's position on the death penalty or contrary to the prohibition on torture.

17.33 There are mechanisms in other legislation requiring that Australia only share certain information with foreign governments if we have a written assurance relating to the information in death penalty proceedings.[969] However, this is not consistent across all legislation. The PJCHR recommended introduction of an express statutory limitation on information sharing specific to *SLAID Act* warrants.[970] The Committee has made similar recommendations in the past for information obtained under various surveillance powers. Such a change would seem consistent with Australia's policy position on both the death penalty and the prohibition on torture (etc.).

17.34 I support the codification of restrictions on sharing information where there is a real risk of the death penalty or torture (etc.). However, this issue is not specific to *SLAID Act* warrants. Indeed, because of the desire to protect the covert capabilities that underpin *SLAID Act* warrants, I consider that it is less likely that information obtained under *SLAID Act* warrants, particularly NAWs, will be shared with most other countries, compared information obtained through more traditional means.[971]

17.35 Any general statutory mechanism to reduce the risk of Australia sharing information that could be used in a death penalty case or in circumstances where there is a real risk of torture (etc.) would be most effective if it was enacted as part of a broader review, such as the current ESR project. Input should also be sought from the Department of Foreign Affairs and Trade on whether such a change would be an effective way to communicate Australia's strong commitment to its position on these issues internationally.

ESR should consider creating a uniform statutory restriction to safeguard against the sharing of information that could reasonably be expected to be used in a manner contrary to Australia's position on the death penalty or the prohibition on torture (etc.).

969 See *TIA Act* sch 1, ss 3(2), (5).

970 *PJCHR Report No 3 2021*, 111 [2.138].

971 For an example of a review that identified problematic sharing see IGIS, *Inquiry into the Actions of Australian Government Agencies in relation to the Arrest and Detention Overseas of Mr Mamdouh Habib from 2001 to 2005* (Public Report, December 2011) <https://webarchive.nla.gov.au/awa/20150304033423/http://www.igis.gov.au/inquiries/docs/habib-inquiry.pdf>.

Chapter 18: Other international obligations

18.1 *SLAID Act* powers raise difficult questions about the prohibition against interfering with the territory or sovereignty of other States, as well as the application of customary international law principles to cyber operations, including in extraterritorial use of law enforcement powers.

18.2 These issues are complex and evolving. They are most likely to arise where an Australian authority interferes with data that is located in another State. This might occur for example by using a DDW to damage or alter data in an offshore server or using an ATW to deprive a person in another country of their ability to access an online account, particularly if that person is a foreign principal or acting on their behalf.

18.3 International police cooperation arrangements, such as those under the *Convention on Cybercrime*, generally call for international cooperation, including on surveillance and data access. This is consistent with longstanding principles for law enforcement activities.

18.4 This chapter briefly outlines Australia's international obligations specific to combating cybercrime. It then considers the application of general non-interference obligations in the context of the use of *SLAID Act* powers. At the moment DDWs and NAWs have limits on non-consensual extra-territorial actions. These guard against breach of non-interference obligations.

18.5 This review did not receive enough evidence to recommend relaxing existing consent requirements – for example, through adding an exception that would allow extraterritorial operation when there was a real risk to safety or other serious harm and where it would not be possible to secure international agreement. There are other existing mechanisms that authorise action outside Australia where cybercrime poses such a threat. Consistent with Australia's current position on DDWs and NAWs, consideration should be given to establishing a consent requirement for ATWs involving the taking over of accounts of people *known* to be outside Australia, unless the service being accessed is hosted in Australia.

18.6 Because this area of international law is still developing, it may be appropriate to revisit these limits in a future review.

International obligations specific to combating cybercrime

18.7 Australia is a party to the *Convention on Cybercrime*. This convention requires the creation of certain cybercrime offences and the enactment of computer interception and search warrants. It also sets out some broad principles about extradition and mutual assistance in cybercrime matters.[972] However, the convention does

[972] *Convention on Cybercrime* arts 19, 21, 24–5.

not oblige Australia to adopt powers akin to those in the *SLAID Act.* Also, it does not provide any authority to unilaterally access data or disrupt data in the territory of another State. To the contrary: it focuses on facilitating police cooperation on cross-border operations.[973]

18.8 The United Nations General Assembly recently adopted the *United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes*.[974] As this convention has not yet opened for signature, it was not considered as an 'international obligation' for the purposes of this review. If Australia were to become a party, in a future review consideration should be given to any obligations that may have relevance to the amendments made by the *SLAID Act*.

Non-interference obligations

18.9 It is a general principle of international law that States should not interfere with the domestic or territorial jurisdiction of other States.[975] It is generally accepted that this principle also applies in cyberspace.[976] In the context of law enforcement, this is generally accepted to mean that a State may only exercise extraterritorial enforcement jurisdiction in relation to persons, objects and cyber activities on the basis of a specific rule of international law or valid consent by the foreign government.[977] A foreign government may grant consent on an ad-hoc basis or pursuant to a treaty.

> Application of traditional principles to the electronic environment is still evolving.

973 See ch III of the *Convention on Cybercrime*. Australia is also a party to a number of international agreements about police cooperation: see, for example, *Agreement on Operation and Strategic Cooperation between Australia and the European Police Office (Europol)*, signed 20 February 2007 [2007] ATS 34 (entered into force 27 September 2007). Australia is also a member of the International Criminal Police Organisation (INTERPOL).

974 *United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes*, GA Res 79/243, UN Doc A/RES/79/243 (24 December 2024).

975 Robert Jennings and Arthur Watts, 'Position of the States in International Law' in Robert Jennings and Arthur Watts (eds), *Oppenheim's International Law: Volume 1 Peace* (9th ed, Oxford University Press, 2008) 428–9; International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Michael Schmitt and Liis Vihul (eds), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017) 315–22 (*Tallinn Manual*).

976 *Tallinn Manual*, 11–12 (Rule 1 – Sovereignty), 55 (Rule 9 – Territorial jurisdiction).

977 Donald Rothwell, Stuart Kaye, Afshin Akhtar-Khavari and Ruth Davis, *International Law: Cases and Materials with Australian Perspectives* (2nd ed, Cambridge University Press, 2014) 294–377; *SS Lotus Case (France v Turkey)* (Judgment) [1927] PCIJ (ser A) No 10, 34–5 [18]–[19].

18.10 The application of these traditional principles to the complexities of an electronic environment has generated controversy and is evolving.[978] There is ambiguity in international law about whether a State may exercise on-line extraterritorial enforcement jurisdiction in circumstances where it is impossible, or difficult, to reliably identify where the data is located.[979] There is also an emerging view that access by law enforcement agencies from within their own territory to 'data that can be accessed on the Internet, but that is not publicly available, such as the content of closed online forums, chat channels, or private Internet hosting services' (even where it is password protected) is a permissible exercise of territorial jurisdiction and does not involve extraterritorial operation, so long as the data is meant to be accessible from the State concerned.[980] This is distinguished from cases where the data is not meant to be accessible to individuals in the State – for example, data stored in a private computer abroad (even if connected to the internet) that is not meant to be accessible.[981] Access to data is not the same as disruption, and disruption or damage to data located in another State is much more likely to be a breach of sovereignty.[982]

Extraterritorial requirements for DDWs and NAWs

18.11 The *SD Act* has some measures that appear intended to reduce the risk of Australia breaching its non-interference obligations, at least in relation to warrants issued under the *SD Act*.[983]

18.12 These provisions apply to NAWs, DDWs and emergency authorisations for a DDW if it becomes 'apparent' to AFP and ACIC that there will be a need for access to, and/or disruption of, data held in a computer in a foreign country. The provisions include a requirement for the applicant agency to obtain consent from 'an appropriate consenting official' of the foreign country to the access and/or disruption. These requirements apply both before a warrant is issued and where extraterritorial operation becomes apparent while a warrant is being executed.[984]

978 Some scholars, having regard to State practice in this area, argue there are new norms of customary international law that may emerge permitting extraterritorial investigative jurisdiction in cyberspace: Cedric Ryngaert, 'Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts' (2023) 24(3) *German Law Journal* 537–50.

979 *Tallinn Manual* 68 [8].

980 *Tallinn Manual* 69–70 [13].

981 *Tallinn Manual* 70 [14].

982 *Tallinn Manual* 18–20 [5],[8],[10]–[14].

983 See AFP, *Submission 18,* 7 [41]; AGD, *Submission 20,* 30.

984 *SD Act* ss 43C(1)-(3), 43E(1)–(3). Where the person executing the warrant is physically present in Australia and the location of the data is not known, or cannot reasonably be determined, the consent of a foreign official is not required: *SD Act* ss 43C(4)(b), 43E(3)(b). Further, evidence obtained from access to or disruption of data in a computer located outside of Australia under a DDW may not be tendered in evidence unless the court is satisfied that consent was granted by the appropriate foreign official: *SD Act* s 43D.

18.13 AFP said that the application of these provisions in practice presented 'one of the most significant challenges in the exercise of these powers' and provided several *hypothetical* examples, including:

- where a person who usually resides in Australia travels to a foreign country for a short period of time and possesses devices that AFP has been lawfully accessing data from in Australia
- where data is held in computers in foreign countries and there is no prospect of obtaining the agreement of a consenting official – for example, where there is no, or poor, foreign relations; or where there is a desire to protect the operational security of the investigation
- where data being stored with cloud hosting services is split across multiple concurrent data centres around the world, requiring separate agreements from consenting officials in multiple countries.[985]

18.14 AGD also said that the agencies often have technical difficulties in determining the location of data online because, for example, 'data is stored in a cloud service which has its physical servers in unknown locations or located across multiple countries.' These trends are accelerated by the 'increased prevalence of technology such as VPNs and proxy servers.'[986]

18.15 These difficulties are mitigated by the fact that consent is presently not required if the location of the data is not known. If the location cannot be determined at the time the warrant application is made, but it is subsequently identified during the life of the warrant, consent must be obtained as soon as it becomes apparent that there will be a need for access to, or disruption of, data held in a computer in a foreign country.[987]

18.16 Evidence provided to this review did include a description of a small number of cases where operations had been affected by the requirement to obtain consent.[988] However, I was advised that AFP and ACIC had no comprehensive records or statistics on how often questions as to extraterritoriality narrow operational plans or may lead to a warrant not being sought. ACIC indicated that none of their NAWs have not proceeded on the basis of the extraterritorial consent requirements.[989] There are clear examples of Australia cooperating with law enforcement bodies in other countries to conduct successful joint operations to combat cybercrime.[990] While the limits on extraterritorial operation may have had some effect, they do not appear to have had a substantial impact on the overall utility of *SLAID Act* warrants which, as discussed in Chapter 2, have been effective.

985 AFP, *Submission 18,* 7–8 [43].
986 AGD, *Submission 20,* 30.
987 *SD Act* ss 43C(3), 43E(2).
988 Details of these cases cannot be published without risk to methodologies and current investigations.
989 Heather Cook, CEO, ACIC, *Public hearing transcript*, 20 February 2025, 58.
990 For example AFP, 'AFP Takes the Fight to Cybercriminals in 2024' (Media Release, 30 December 2024); AFP, 'AFP Joins Global Crackdown on Cybercriminal Infrastructure Provider' (Media Release, 12 February 2025); AFP, 'AFP Urge Victims to Report Cybercrime Following Ransomware Disruption' (Media Release, 31 October 2022). These operations did not necessarily involve the use of *SLAID Act* warrants and are included as general examples of international police cooperation on cybercrime.

18.17 Given the uncertain state of international law in this area, and the fact that Australia is unlikely to want other States using *SLAID Act* like powers on infrastructure that is inside Australia, caution is needed when considering removing the extraterritorial limits on *SLAID Act* powers. Both AGD and AFP have recognised this. AGD said, 'it is challenging to have a legislative provision that itself resolves extraterritorial and international law issues.'[991] AFP agreed that there are limited legislative options for addressing operational barriers resulting from the requirement to obtain consent.[992]

18.18 I acknowledge that in certain cases AFP and ACIC may face difficulties in obtaining the required consent where it is known that the data to be accessed or disrupted is held in a foreign country. However, I do not consider that agencies made a sufficient case to justify a departure from the existing consent requirements, particularly noting the role that these play in ensuring compliance with Australia's international law obligations. There are also other options available in critical cases.[993]

In certain cases, there may be difficulties in obtaining consent. However, information provided to this review did not support the removal of consent requirements at this time. Because of evolving technology and developing international law in this area, it may be appropriate to re-examine this position in future inquiries.

Extraterritorial operation of ATWs

18.19 In contrast to DDWs and NAWs, the *Crimes Act* does not require consent where an ATW involves access to an account or data located in a foreign country. This approach is seemingly based on the *physical* search related powers in the *Crimes Act*. Physical searches conducted in Australia do not raise the same concerns about compliance with non-interference obligations.[994] In so far as *Crimes Act* search warrants allow access to data that is accessible from computers found on the searched premises,[995] the risk of interference arising from this access is much lower than for the taking over of an account under an ATW, particularly one not used by a person in Australia or not used to access an Australian service. The ATW power is not akin to the physical search that *Crimes Act* warrants are premised on. An ATW allows more than access to data and will usually result in AFP or ACIC having *exclusive* access to an account, thereby potentially depriving a person in another country of their ability to access their online account.

991 Sarah Chidgey, Deputy Secretary, AGD, *Public hearing transcript*, 20 February 2025, 69.
992 Ian McCartney, Deputy Commissioner, AFP, *Public hearing transcript*, 20 February 2025, 36.
993 The *IS Act* makes it clear that in certain situations the Australian Government intends ASD to undertake cyber disruption and intelligence collection actives *outside* Australia: see s 7(1)(a), (c). This does not give ASD authority to disrupt or access data on computers *inside* Australia – doing so would be contrary to the cyber offences in the *Criminal Code* and would not be covered by the immunity in s 14 of the *IS Act*.
994 Special rules apply to diplomatic persons and premises: *Vienna Convention on Diplomatic Relations* opened for signature 18 April 1961, 500 UNTS 95 (entered into force 24 April 1964) and *Diplomatic Privileges and Immunities Act 1967* (Cth).
995 *Crimes Act* s 3L.

18.20 AGD said that the absence of an extraterritorial restriction on ATWs is appropriate because ATWs 'only allow access to an account, additional warrants or authorisations are required for other activities related to the account, each of which contain their own frameworks regarding extraterritoriality.'[996] It is not clear that this is always so. For example, if operation of an account that has been taken over using an ATW is to be authorised under a controlled-operation authority, there does not appear to be any requirement for consent for extraterritorial activity.[997] If a computer access warrant is to be used, there is a requirement for consent if it is known that data is outside Australia.[998] In this case, consent to take over the account could presumably be sought at the same time.

18.21 Australia's position on ATWs appears to be inconsistent with the current position for DDWs, NAWs and computer access warrants. Consideration should be given to introducing a consent requirement for ATWs, at least where the account is intended to access a service located outside Australia and the account user is known to be outside Australia.

> Consideration should be given to introducing a consent requirement where the account being accessed under an ATW is held in a foreign country.

18.22 I have made this a suggestion rather than a specific recommendation for legislative reform, as I recognise that further consultation within government is needed for the executive to reach a view on Australia's position on the still-developing international law in this area. At the very least, this inconsistent position potentially raises foreign relations risks for Australia that need to be managed by the appropriate area within government.

Management of foreign relations risks

18.23 In addition to the risk that arises from the inconsistent position on ATWs, there is foreign relations risk in any *SLAID Act* operation that has extraterritorial effect – including where consent is obtained but there are unintended consequences or where consent is not obtained because, when the operation is undertaken, it is not known where the data is located.

996 AGD, *Submission 20*, 30.

997 This is not surprising, as the controlled operation scheme is clearly directed to physical activity that occurs in Australia for which immunity from civil or criminal liability may be needed: see pt IAB of the *Crimes Act* and, in particular, s 15G (Objects of Part) and ss 15HA–15HB (Protection from criminal responsibility for controlled conduct during controlled operations; Indemnification of participants against civil liability).

998 *SD Act* s 43A.

18.24 One element of the current threat environment is an elevated risk from global state sponsored cyber activity as geopolitical circumstances change. Dr Walker-Munro and the Queensland Council for Civil Liberties cautioned that AFP or ACIC 'conducting aggressive cyber activities' outside Australia raises a risk the use of these powers 'will create an international diplomatic or foreign policy incident when a computer, network or system outside of Australia's sovereign territory is impacted by such a power.'[999] More generally, because the effects of cybercrime may be spread across different jurisdictions, there is also the risk that multiple law enforcement agencies located across different jurisdictions will take overlapping enforcement action on the same threat.

18.25 Dr Walker-Munro suggested that there should be a legislative or policy requirement for AFP or ACIC to obtain the advice of the Minister for Foreign Affairs and Trade before 'undertaking a warrant operation that may have international diplomatic or foreign policy ramifications.'[1000]

18.26 Arrangements for engaging the Minister for Foreign Affairs and Trade and their portfolio in assessing foreign relations risk have been previously considered in the context of other reviews, including the 2019 Comprehensive Review.[1001] That Review concluded that there was a need for improved consultation processes between agencies and the Department of Foreign Affairs and Trade; however, it was considered that this was not best achieved through legislation or a prescriptive framework.[1002]

18.27 I agree with this conclusion. I consider that foreign relation risks relating to the use of *SLAID Act* powers would be better addressed through administrative arrangements that ensure prompt consultation with the Department of Foreign Affairs and Trade and their Minister in appropriate circumstances.

> Foreign relations risks should be managed through administrative arrangements between the Department of Foreign Affairs and Trade, AFP and ACIC.

999 Brendan Walker-Munro, *Submission 3*, 5. QCCL considered that definitional concepts like 'computer' should be narrowed to minimise risk of extraterritorial operation: QCCL, *Submission 6*, 7–8.

1000 Brendan Walker-Munro, *Submission 3*, 6. There is an existing requirement to provide the Minister with responsibility for the *SD Act* with evidence that access to data and/or disruption of data has been agreed to by an appropriate consenting official where such consent is required: *SD Act* ss 43C(7), 43E(6).

1001 The 2019 Comprehensive Review's consideration of this issue was focused on the activities of ASIO, Australian Secret Intelligence Service and ASD on the basis that the offshore activities of AFP and ACIC were seen as carrying less risk as were 'declared or otherwise overt, and conducted in cooperation with the foreign country in which they are operating': *2019 Comprehensive Review* vol 1, 351 [16.27]. Note that this preceded the introduction of the *SLAID Act* powers.

1002 *2019 Comprehensive Review* vol 1 355 [16.49].

Acronyms and abbreviations

Term	Meaning
2019 Comprehensive Review	Dennis Richardson, *Report of the Comprehensive Review of the Legal Framework of the National Intelligence Community* (Final Report, December 2019)
2024 INSLM Secrecy Review	Jake Blight, INSLM, *Secrecy Offences – Review of Part 5.6 of the Criminal Code 1995* (Report, 27 June 2024)
2024 Independent Intelligence Review	Commonwealth of Australia, Department of the Prime Minister and Cabinet, *2024 Independent Intelligence Review* (Report, 21 March 2025) X.
AAT	Administrative Appeals Tribunal
ACIC Review	Stephen Merchant and Greg Wilson, *Independent Review of the Australian Criminal Intelligence Commission and associated Commonwealth law enforcement arrangements* (Report, May 2024)
ART	Administrative Review Tribunal
ART Act	*Administrative Review Tribunal Act 2024* (Cth)
ATW	*Account takeover warrant*
Convention on Cybercrime	*Convention on Cybercrime*, opened for signature 23 November 2001, [2013] ATS 9 (entered into force 1 July 2004)
DDW	Data disruption warrant
ESR	Electronic surveillance reform
Government response to the 2019 Comprehensive Review	Australian Government, *Commonwealth Government response to the Comprehensive Review of the Legal Framework of the National Intelligence Community* (Government Response, December 2020)
ICCPR	*International Covenant on Civil and Political Rights,* opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976).
IPCO	United Kingdom Investigatory Powers Commissioner's Office
IS Act	*Intelligence Service Act 2001* (Cth)

Term	Meaning
LPP	Legal professional privilege
NAW	Network activity warrant
NSW SD Commissioner	New South Wales Surveillance Devices Commissioner
Operation Prospect Report	Acting NSW Ombudsman, *Operation Prospect: A special report to Parliament under s 31 of the Ombudsman Act 1974 and s 161 of the Police Act 1990* (Report, December 2016)
PIM	Public interest monitors
PJCIS SLAID Report	PJCIS, Parliament of Australia, *Advisory report on the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (Report, August 2021)
PJCLE Cybercrime Review	Inquiry into the capability of law enforcement to respond to cybercrime
Revised Explanatory Memorandum	Revised Explanatory Memorandum, Surveillance Legislation Amendment (Identify and Disrupt) Bill 2021 (Cth)
Scrutiny of Bills Committee	Senate Standing Committee for the Scrutiny of Bills
SD Act	*Surveillance Devices Act 2004* (Cth)
SLAID Act	*Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* (Cth)
SLAID Bill	Surveillance Legislation Amendment (Identify and Disrupt) Bill 2021 (Cth)
Supplementary Explanatory Memorandum	Supplementary Explanatory Memorandum, Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020
TAP	United Kingdom Technology Advisory Panel
TIA Act	*Telecommunications (Interception and Access) Act 1979* (Cth)
TOLA Act	*Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth)
TSOC	Transnational, serious and organised crime

List of submissions

Submissions in response to Issues Paper

No	Organisation or individual	Date received	Reference
01	Marcus Smith	12 November 2024	Marcus Smith, *Submission 1*
02	NSW Surveillance Devices Commissioner	6 December 2024	NSW SD Commissioner, *Submission 2*
03	Dr Brendan Walker-Munro	12 December 2024	Brendan Walker-Munro, *Submission 3*
04	Civil Liberties Australia	12 December 2024	Civil Liberties Australia, *Submission 4*
05	Human Rights Law Centre	17 December 2024	HRLC, *Submission 5*
06	Queensland Council for Civil Liberties	18 December 2024	QCCL, *Submission 6*
07	Alliance for Journalists' Freedom	18 December 2024	AJF, *Submission 7*
08	Dr Philip Glover	18 December 2024	Philip Glover, *Submission 8*
09	Inspector-General of Intelligence and Security	18 December 2024	IGIS, *Submission 9*
10	New South Wales Council for Civil Liberties	18 December 2024	NSWCCL, *Submission 10*
11	Commonwealth Ombudsman	18 December 2024	Ombudsman, *Submission 11*
12	Australian Information Industry Association	19 December 2024	AIIA, *Submission 12*
13	Public Interest Monitor – Queensland	19 December 2024	Qld PIM, *Submission 13*
14	Uniting Church in Australia, Synod of Victoria and Tasmania	19 December 2024	Uniting Church in Australia, Synod of Victoria and Tasmania, *Submission 14*

No	Organisation or individual	Date received	Reference
15	Joint Submission – Associate Professor Rebecca Ananian-Welsh, Associate Professor Tamara Tulich, Dr Keiran Hardy, Professor Peter Greste, Dr Ausma Bernot & Associate Professor Danielle Ireland-Piper	20 December 2024	Joint Academic Submission, *Submission 15*
16	Internet Association of Australia	19 December 2024	IAA, *Submission 16*
17	Australian Criminal Intelligence Commission	20 December 2024	ACIC, *Submission 17*
17a	Australian Criminal Intelligence Commission	20 December 2024	ACIC, *Submission 17a* (classified)
18	Australian Federal Police	20 December 2024	AFP, *Submission 18*
19	Media Entertainment and Arts Alliance	10 January 2025	MEAA, *Submission 19*
20	Attorney-General's Department	15 January 2025	AGD, *Submission 20*
20a	Attorney-General's Department	15 January 2025	AGD, *Submission 20a* (classified)
21	Australian Human Rights Commission	20 January 2025	AHRC, *Submission 21*
22	Digital Rights Watch	23 January 2025	Digital Rights Watch, *Submission 22*
23	Law Council of Australia	28 January 2025	Law Council, *Submission 23*
24	Public Interest Monitor – Victoria	30 January 2025	Victorian PIM, *Submission 24*

Supplementary submissions and responses following public hearing

No	Organisation or individual	Date received	Reference
25	NSW Surveillance Devices Commissioner	4 March 2025	NSW SD Commissioner, *Supplementary submission 25*
26	Law Council of Australia	4 March 2025	Law Council, *Supplementary response 26*
27	Dr Philip Glover	6 March 2025	Philip Glover, *Supplementary submission 27*
28	Attorney-General's Department	6 March 2025	AGD, *Supplementary submission 28*
29	Australian Federal Police	18 March 2025	AFP, *Supplementary response 29*

Annex A: Review methodology

The *Independent National Security Legislation Monitor Act 2010* (Cth) (*INSLM Act*) provides considerable scope for each Monitor to determine the process for each review conducted under that Act.

This review began July 2024. Initial meetings with government and non-government stakeholders together with independent research and analysis led to the production of a detailed issues paper being released in November 2024. Throughout the course of the review the Monitor and INSLM staff had many constructive meetings with stakeholders. The Monitor also convened a roundtable meeting in December 2024 to provide a forum for the sharing of ideas and to test preliminary views.

The Monitor used the powers available in Part 3 of the *INSLM Act* to require the Australian Federal Police (AFP) and the Australian Criminal Intelligence Commission (ACIC) to provide certain information and documents. As explained in the body of this report the use of these powers was necessary to override the secrecy offences introduced by the *SLAID Act* which may have otherwise prevented the agencies providing information relevant to this review. It does not reflect any lack of cooperation by the agencies with the review.

A public hearing was held in February 2025, and private hearings with AFP and ACIC were held in July 2024 and March 2025. The Monitor invited supplementary submissions following the public hearings and had a number of follow-up meetings.

Prior to the report being finalised, AFP and ACIC were consulted about text in the report that draws on information that they provided in classified submissions, private hearings or in response to orders to produce information or documents. The purpose of that consultation was to assist the Monitor in ensuring that the report does not include information of the type described in s 29(3) of the *INSLM Act*. A copy of this report was provided to the Attorney-General on 31 July 2025.

Issues Paper

On 7 November 2024 the Monitor wrote to a broad range of stakeholders to provide them with a copy of the Issues Paper for this review. The issues paper was also made available on the INSLM website. The 75-page paper provided detailed background and analysis of the powers introduced by schedules 1, 2 and 3 of the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* (Cth) (*SLAID Act*). Without limiting the scope of discussion and review, the issues paper asked 22 specific questions arising from analysis of the *SLAID Act*. The paper was also accompanied by a compilation of hypothetical case studies on the use of each warrant.

Roundtable

On 4 December 2024, the Monitor convened a roundtable with key experts and stakeholders to discuss their preliminary views on the warrants and associated powers introduced by the *SLAID Act*. In addition to INSLM staff, the participants were:

- Dr Brendan Walker-Munro – Southern Cross University
- Dr Dominique Dalla-Pozza – The Australian National University
- Dr Gregor Urbas – The Australian National University
- Dr Kristine Klugman – Civil Liberties Australia
- Dr Monique Mann – Victoria University Wellington
- Dr Philip Glover – Edith Cowan University
- Dr Sarah Kendall – University of Queensland
- Dr William Stolz – The Australian National University
- Angus Murray – Queensland Council for Civil Liberties
- Lizzie O'Shea – Digital Rights Watch
- Lloyd Babb SC – Law Council of Australia
- Shounok Chatterjee – Law Council of Australia (observer)
- Stephen Banks – New South Wales Council for Civil Liberties

A summary of the roundtable was published on the INSLM website.

Consultation and private meetings

The Monitor spoke with many individuals and organisations about the *SLAID Act* warrants between May 2024 and July 2025. Consultations were held in-person in Brisbane, Sydney, Canberra and Melbourne, via phone and online. These included meetings with AFP, ACIC, the Attorney-General's Department, the Department of Home Affairs, the Commonwealth Ombudsman, the Inspector-General of Intelligence and Security, the Administrative Review Tribunal, Judges and Registrars. The Monitor and INSLM staff also met with State police, Public Interest Monitors and the NSW Surveillance Devices Commissioner. In addition, the Monitor met with civil society groups including the Law Council of Australia and Queensland Council for Civil Liberties.

Where they have been specifically relied on in this report, records of relevant conversation were agreed in correspondence.

Submissions

The Monitor received 26 submissions (including 2 classified submissions) in response to the Issues Paper. Following the hearing there were an additional 5 supplementary submissions as well as responses to questions on notice from 3 agencies. Almost all submissions, supplementary submissions and questions on notice responses were made publicly available on the INSLM website. A small amount of material was provided in classified annexes or otherwise identified as not suitable for publication by the agencies providing it.

Public hearing

A public hearing was held on 19 and 20 February March 2025 in Canberra. A live stream of the hearing was available and a transcript and recording of the hearing is published on the INSLM website.

Representatives appeared from the following government agencies:

- ACIC
  - Ms Heather Cook – Chief Executive Office
  - Mr Matthew Rippon – Deputy CEO, Intelligence
  - Ms Nicole Mayo – Chief Counsel/Executive Director, Legal and Assurance
  - Ms Wendy Darling – National Manager, Collection Operations
- AFP
  - Mr Ian McCartney – Deputy Commissioner, Crime
  - Ms Alison Wegg – Assistant Commissioner, Intelligence and Covert Services
  - Mr Richard Chin – Assistant Commissioner, Cyber Command
  - Mr Rob Nelson – Commander, Covert and Technical Operations
- Attorney-General's Department
  - Ms Sarah Chidgey PSM – Deputy Secretary, National Security and Criminal Justice Group
  - Mr Parker Reeve – A/g First Assistant Secretary, Criminal Justice Division
- Australian Human Rights Commission
  - Dr Lorraine Finlay – Human Rights Commissioner

Non-government witnesses were:

- Academic
  - Dr Philip Glover – Lecturer in Law, Edith Cowan University

- Academic Forum
  - Associate Professor Rebecca Annanian-Welsh – TC Beirne School of Law, University of Queensland
  - Associate Professor Keiran Hardy – Griffith Criminology Institute, Griffith University
  - Dr Ausma Bernot – Lecturer in Technology & Crime, Griffith Criminology Institute, Griffith University
- Australian Information Industry Association
  - Ms Siew Lee Seow – General Manager, Policy and Media
- Australian Privacy Foundation
  - Dr Monique Mann – Vice Chair
- Human Rights Law Centre
  - Mr Kieran Pender – Associate Legal Director
  - Ms Anneliese Cooper – Lawyer
- Internet Association of Australia
  - Ms Narelle Clark – Chief Executive Officer
  - Ms Sophia Joo – Policy Officer
- Law Council of Australia
  - Mr Lloyd Babb SC – Chair of the Law Council's National Security Law Working Group
  - Mr Tim Game SC – Member of the Law Council's National Security Law Working Group
  - Mr Nathan MacDonald – Deputy General Manager, Policy Division
- Media Entertainment and Arts Alliance
  - Ms Karen Percy – Media Section President
- NSW Council for Civil Liberties
  - Mr Stephen Blanks – Treasurer
- Queensland Council for Civil Liberties
  - Mr Angus Murray – Vice President

Private hearing

Private hearings were held on 23, 29 July 2024 and 11 March 2025. A summary of each hearing was published on the INSLM website.

Annex B: Duty of candour in other Five Eyes jurisdictions

This annexure contains a summary of the standard of disclosure (either as a matter of common law or administrative practice) imposed on warrant applications for electronic surveillance powers in New Zealand, Canada, United Kingdom and United States. There are several examples in these jurisdictions where courts or oversight bodies have identified non-compliance with the relevant standard of disclosure which are also outlined below.

Duty of candour or equivalent standard of disclosure

Jurisdiction	Duty of candour or equivalent standard of disclosure
New Zealand	There is an 'extensive and demanding' common law duty of candour where '… failure to discharge that duty, notwithstanding good faith, may render a warrant invalid or unlawful.'[1] This duty is a 'particular application' of the general principles that apply in ex parte proceedings and operates alongside complementary statutory provisions.[2] The warrant applicant is obliged to set out in their evidence supporting the warrant application '… all matters known to the applicant which might be relied on by the target of the warrant if that person had the opportunity to appear in opposition.'[3] The New Zealand Inspector General of Intelligence and Security has said that:[4] *The duty requires them to set forth any matters of fact or law that, if brought to the attention of the decision-maker, might be material to whether the warrant should be issued, what may be done under it, and whether conditions should be imposed. An applicant must be careful not to decide themselves what the decision-maker "needs to know", and must bear in mind that a warrant is a prescriptive permission, not a high-level licence.*

1 *Hager v Attorney-General* [2015] NZHC 3268, [68].
2 *Hager v Attorney-General* [2015] NZHC 3268, [62-63]. Complementary statutory provisions include, for example, the requirement for an search warrant application to be accompanied by a statement that the application is true and accurate: *Search and Surveillance Act 2012* (NZ) s 99.
3 *Tranz Rail Ltd v Wellington District Court* [2002] 3 NZLR 780, [21] citing *R v McColl* (1999) 17 CRNZ 136, 142–143.
4 Office of the Inspector-General of Intelligence and Security (New Zealand), Annual Report: For the year 1 July 2018 to 30 June 2019 (Report, 5 November 2019) 8–9.

Jurisdiction	Duty of candour or equivalent standard of disclosure
Canada	The common law duty of full and frank disclosure that applies in ex parte proceedings applies in the context of a warrant applications in Canada. The Canadian Supreme Court has said that this duty requires that '[t]he evidence presented must be complete and thorough and no relevant information adverse to the interest of that party may be withheld.'[5] The duty of candour also requires '… an ongoing effort to update, throughout the proceedings, the information and evidence …' regarding the subject of the without notice application.[6] The Canadian Federal Court considered that the obligations and responsibilities flowing from the duty of candour in the context of warrant applications were not limited to the individuals who appear before the Court and extended to those in leadership positions within the applicant agency.[7]
United Kingdom	The common law duty of candour that applies to applications made to a court without notice applies 'equally to the duty of an applicant for a search warrant'. [8] That duty requires 'full and accurate disclosure to the court, including disclosure of anything that might militate against the grant.'[9] This standard has also been described by the United Kingdom Supreme Court in terms that '… the information on which [the warrant applicant] relies must constitute a fair and balanced presentation of the circumstances on the basis of which a warrant is sought.'[10]

5 *Ruby v Canada (Solicitor General)* [2002] 4 SCR 3, [27]; *Canada (Citizenship and Immigration) v Harkat* [2014] 2 SCR 33, [101].

6 *Canada (Citizenship and Immigration) v Harkat* [2014] 2 SCR 33 [102].

7 *In the Matter of an application for a warrant under sections 12 and 21 of the Canadian Security Intelligence Service Act, RSC 1985, c C-23 (Re)* [2020] FC 616, [89].

8 *Chatwani & Ors, R (on the application of) v The National Crime Agency & Anor* [2015] EWHC 1283 (Admin) (11 May 2015), [106].

9 *Chatwani & Ors, R (on the application of) v The National Crime Agency & Anor* [2015] EWHC 1283 (Admin) (11 May 2015), [106], citing *Energy Financing Team Limited v The Director of the Serious Fraud Office* [2005] EWHC 1626 (Admin); *R (Golfrate Property Management Limited) v The Crown Court at Southwark* [2014] EWHC 840 (Admin), [24]–[27]; *In re Stanford International Bank Limited* [2010] EWCA Civ 137, [191].

10 *R (on the application of Haralambous) v Crown Court at St Albans and another* [2018] UKSC 1, 20 [34].

Jurisdiction	Duty of candour or equivalent standard of disclosure
United States	There are binding internal policies that effectively require a duty of candour. These are supported by factual accuracy review procedures ('Woods Procedures') for *Foreign Intelligence Surveillance Act*, 50 U.S.C. §§ 1801, 1821 et seq. (1978) ('*FISA*') applications. In broad terms, the Woods Procedures are intended to minimise factual inaccuracies in *FISA* applications and to ensure that statements contained in applications are 'scrupulously accurate'. The Woods Procedures require internal documentation to support each factual assertion contained in an application. Additionally, FBI agents are required to sign a declaration affirming that each factual statement in the application is accurate and supported by documentation in the Woods File.[11]

Examples of non-compliance with the relevant disclosure standard

New Zealand

The New Zealand IGIS has made a number of findings pertaining to lack of compliance with the duty of candour in recent years, including in the following contexts: when it is appropriate for there to be conditions in a warrant; the likelihood of intercepting privileged communications; the role of parties assisting with the execution of a warrant; where a known purpose in seeking the warrant is to share information with certain third parties; where the agencies know there are limitations on their ability to minimise collection of incidental information or to control access to information after it has been shared with other agencies.[12]

11 Department of Justice, Office of the Inspector General, *Audit of the Federal Bureau of Investigation's Execution of Its Woods Procedures for Applications Filed with the Foreign Intelligence Surveillance Court Relating to U.S. Persons* (Report, September 2021).

12 See for example: Office of the Inspector-General of Intelligence and Security (New Zealand), *Annual Report: For the year 1 July 2018 to 30 June 2019* (Report, 5 November 2019) 8–9.

Canada

The Canadian Federal Court found the duty of candour had not been complied with by the Canadian Security Intelligence Service in failing to disclose information that was likely illegally obtained. The Federal Court observed that the Department of Justice 'must identify and implement the institutional structures and processes necessary to ensure individual and institutional compliance with the duty'.[13] Since that decision further guidance regarding the scope of the duty has been provided.[14]

United Kingdom

In 2023 the United Kingdom Investigatory Powers Division Tribunal considered that 'where MI5 is aware of serious and longstanding issues of non-compliance with statutory safeguards, there is a duty to bring that to the attention of the (Secretary of State) when seeking a warrant'.[15] In that case, the issues of non-compliance were well-known to MI5 for some time and pertained to retention, review and disposal of personal data within MI5's technology environments.

United States

In the United States, the 2021 Audit of the Federal Bureau of Investigation's Execution of Its Woods Procedures for Applications Filed with the Foreign Intelligence Surveillance Court Relating to U.S. Persons conducted by Department of Justice Inspector General Michael E. Horowitz ('the Horowitz Review')[16] investigated the FBI's compliance with the Woods Procedures for *FISA* applications.

Relevantly, the Horowitz Review reviewed a sample of 29 applications and found over 400 instances of non-compliance with the Woods Procedures, with 4 breaches considered 'material' to the assessment of probable cause.[17] Those material errors included:

13 *In the matter of an application for a warrant under sections 12 and 21 of the Canadian Security Intelligence Service Act, RSC 1985, c C-23 (Re)* [2020] FC 616, [89].

14 In 2020, The Canadian Federal Court recommended comprehensive external review to identify systemic changes to address non-compliance with the duty of candour: *Sections 12 and 21 of the Canadian Security Intelligence Service Act, RSC 1985, c C-23 (Re)* [2020] FC 616; Canada, National Security and Intelligence Review Agency, *Rebuilding Trust: Reforming the CSIS Warrant and Justice Legal Advisory Processes – NSIRA Review arising from Federal Court's Judgment in 2020 FC 616* (Report, 16 June 2022).

15 *Liberty v Security Service* [2023] UKIPTribl 1, 35 [135].

16 Department of Justice, Office of the Inspector General, *Audit of the Federal Bureau of Investigation's Execution of Its Woods Procedures for Applications Filed with the Foreign Intelligence Surveillance Court Relating to U.S. Persons* (Report, September 2021).

17 Department of Justice, Office of the Inspector General, *Audit of the Federal Bureau of Investigation's Execution of Its Woods Procedures for Applications Filed with the Foreign Intelligence Surveillance Court Relating to U.S. Persons* (Report, September 2021) 19.

- where a *FISA* warrant application referred to statements made by the target of the surveillance in support of a referenced organisation, '[f]ailing to include context' that suggested those remarks 'were made … to provoke a response from law enforcement personnel';
- failing to provide evidence in the Woods File providing further context that the target's support for a specific group instead indicated support for a cause;
- describing the target's use of a financial account as at a certain date without providing context regarding how recently the government has confirmed the target's use of that account.[18]

[18] Department of Justice, Office of the Inspector General, *Audit of the Federal Bureau of Investigation's Execution of Its Woods Procedures for Applications Filed with the Foreign Intelligence Surveillance Court Relating to U.S. Persons* (Report, September 2021) 11.